HP Server Automation

Ultimate Edition

ソフトウェアバージョン: 10.10

概要とアーキテクチャー

ドキュメントリリース日: 2014年6月30日 (英語版)
ソフトウェアリリース日: 2014年6月30日 (英語版)

ご注意

保証

HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

商標について

Adobe®は、Adobe Systems Incorporated (アドビシステムズ社)の登録商標です。

Intel®およびItanium®は、Intel Coporationの米国およびその他の国における登録商標です。

Microsoft®、Windows®、およびWindows® XPは，Microsoft Corporationの米国における登録商標です。

OracleとJavaは、Oracle Corporationおよびその関連会社の登録商標です。

UNIX®は、The Open Groupの登録商標です。

サポート

次のHPソフトウェアサポートオンラインのWebサイトを参照してください。

http://support.openview.hp.com

このサイトでは、HPのお客様窓口のほか、HPソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HPソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HPサポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、HP Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport IDを登録するには、次のWebサイトにアクセスしてください。

http://h20229.www2.hp.com/passport-registration.html

アクセスレベルの詳細については、次のWebサイトをご覧ください。

http://support.openview.hp.com/access_level.jsp

サポートマトリクス

サポートおよび互換性情報については、関連する製品リリースのサポートマトリクスを参照してください。サポートマトリクスと製品マニュアルは、次のHPソフトウェアサポートオンラインのWebサイトで参照できます。

http://h20230.www2.hp.com/sc/support_matrices.jsp

また、本リリースの『HP Server Automation Support and Compatibility Matrix』は、次のHPソフトウェアサポートオンラインの製品マニュアルWebサイトからダウンロードできます。

http://h20230.www2.hp.com/selfsolve/manuals

ドキュメントの更新情報

このリリースのServer Automation製品の最新のドキュメントは、すべて次のSA Documentation Libraryから入手できます。

http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

SA Documentation Libraryでは、このリリースに関連するガイドライン、リリースノード、サポートマトリクス、およびホワイトペーパーにアクセスできます。また、フルドキュメントセットを一括してダウンロードすることもできます。SA Documentation Libraryは、リリースごとに更新されます。また、リリースノートが更新されたときや、新しいホワイトペーパーが発行されたときにも更新されます。

情報リソースを見つける方法

Server Automationの情報リソースは、次のいずれの方法でもアクセスできます。

方法1: 新しいSA Documentation Libraryから、最新のドキュメントにタイトルとバージョンを指定してアクセスします。

方法2: [All Manuals Download] からローカルディレクトリにフルドキュメントメントセットを保存します。

方法3: サポートされるリリースのHP製品ドキュメントをHPソフトウェアドキュメントポータルで検索します。

各ドキュメントにアクセスするには、次の手順を実行します。

1. SA 10.x Documentation Libraryにアクセスします。

   http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

2. HP Passportの資格情報を使ってログインします。
3. ドキュメントのタイトルとバージョンを指定して、[**go**] をクリックします。

ローカルディレクトリ内の完全なドキュメントセットを使用するには、次の手順を実行します。

1. フルドキュメントセットをローカルディレクトリにダウンロードするには、次の手順を実行します。
   a. SA Documentation Libraryにアクセスします。

      http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

b HP Passportの資格情報を使ってログインします。

c SA 10.1バージョンの [All Manuals Download] タイトルを探します。

d [**go**] リンクをクリックして、ローカルディレクトリにZIPファイルをダウンロードします。

e ファイルを解凍します。

2 ローカルディレクトリ内のドキュメントを探すには、ドキュメントカタログ (docCatalog.html) を使用します。ローカルディレクトリにダウンロードしたドキュメントの索引ポータルが表示されます。

3 ドキュメントセット内のすべてのドキュメントを対象としてキーワードを検索するには、次の手順を実行します。

a ローカルディレクトリ内の任意のPDFドキュメントを開きます。

b [**編集**] > [**高度な検索**] を選択します (またはShift＋Ctrl＋Fキー)。

c [以下の場所にあるすべてのPDF文書] オプションを選択し、ローカルディレクトリを指定します。

d キーワードを入力し、[検索] をクリックします。

HPソフトウェアドキュメントポータルで追加ドキュメントを探すには、次の手順を実行します。

HPソフトウェアドキュメントポータルにアクセスします。

http://h20230.www2.hp.com/selfsolve/manuals

このサイトを利用するには、HP Passportへの登録とサインインが必要です。HP Passport IDの登録は、HP Passportのサインインページの [**New users - please register**] リンクをクリックしてください。

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HPの営業担当にお問い合わせください。改訂状況については、「ドキュメントの更新情報」を参照してください。

製品エディション

Server Automationには、次の2つの製品エディションがあります。

- Server Automation (SA) は、Server AutomationのUltimate Editionです。Server Automationについては、『SAリリースノート』および『SAユーザーガイド: Server Automation』を参照してください。
- Server Automation Virtual Appliance (SAVA) は、Server Automation の Premium Edition です。SAVA の機能については、『SAVA Release Notes』および『SAVAクイックガイド』を参照してください。

目次

第1章 Server Automationの概要

Server Automationの概要

本項では、Server Automation (SA) の基本機能とアーキテクチャーについて説明します。SAの詳細については、第3章「SAアーキテクチャーの詳細」を参照してください。

SAは、データセンター自動化ソフトウェアであり、次に示すように、さまざまなデータセンター機能の一元管理と合理化、データセンターで実施されるサーバー管理の中で重要な分野の自動化を行います。

- **サーバー検出**

  SA はネットワークをスキャンして管理対象になっていないサーバーを検出し、エージェントレスサーバーリストに表示します。そこで、リストに表示されたこれらのサーバーのそれぞれにSAエージェントをインストールして、SAの管理下に置きます。SAの管理対象のサーバーでは、次に示す管理タスクを実行できます。

  — **オペレーティングシステムのプロビジョニング**

  SAのOSプロビジョニングでは、ベアメタルサーバーと仮想サーバーのプロビジョニングを事前構成されたオペレーティングシステムを使用して行います。新しくプロビジョニングされたサーバーはSA管理対象サーバープールに追加され、SAによる一元管理が可能になります。

  — **オペレーティングシステムのパッチ適用**

  SA では、Windows、Linux、Solarisベースの管理対象サーバーにオペレーティングシステムパッチを適用します。パッチは集中管理され、柔軟かつ自動的に適用されます。適用が必要なパッチを、オペレーティングシステムベンダーが認定したパッチリストと照合することができます。また、適用プロセスのカスタマイズによって、サーバー環境と互換性のないパッチを除外することも可能です。

  — **ソフトウェアのプロビジョニング**

  サーバーを管理対象サーバープールに追加したら、ソフトウェアポリシーと呼ばれるテンプレートを使用してソフトウェアアプリケーションのインストールと構成を実行します。ソフトウェアポリシーでは、インストールするソフトウェア、適用する構成、インストール時に実行するスクリプトが定義されています。ソフトウェアポリシーを使用することにより、サーバーのベースライン構成を作成し、これを SA のソフトウェアコンプライアンス機能で適用することが可能です。たとえば、Apacheサーバーのベースラインバージョンを作成し、これをSA管理対象サーバーのすべてまたは一部にインストールできます。

  — **監査とコンプライアンス**

  SA の監査と修復では、サーバー構成ポリシーを定義して、このポリシーの基準に SA 管理対象サーバーが準拠していることを確認します。非コンプライアンス状態 (想定通りに構成されていない状態) のサーバーが検出された場合、修復 (強制的に準拠した状態にする処理) が可能です。コンプライアンスポリシーは、すべてのサーバーの構成基準として指定したベースサーバーのスナップショットを元に作成できます。

  SA の監査証跡データは、データセンター環境において、Sarbanes-Oxley 法、Gramm-Leach-Bliley 法 (GLB法)、Health Information Portability and Accountability Act (HIPAA) などでますます急務となる厳格なアカウンタビリティを確保する上で役立ちます。

— **アプリケーション構成**

アプリケーション構成テンプレートを設計し、これをすべてのSA管理対象サーバーにプッシュします。たとえば、Apache Webサーバーがあり、すべてのサーバーの構成ファイルを標準化したい場合には、アプリケーション構成を使用すると便利です。詳細については、『SAユーザーガイド: アプリケーション構成』を参照してください。

— **アプリケーションデプロイメント**

SAのアプリケーションデプロイメントでは、カスタマイズされた複雑な多層アプリケーションを、開発チームから品質保証チームに簡単かつ迅速に移動できます。アプリケーションは、テスト、運用準備、ステージング、最終的には運用開始へと移動します。詳細については、『SA User Guide: Application Deployment Manager』を参照してください。

— **ソフトウェアコンプライアンス**

SAのソフトウェアポリシーのコンプライアンススキャンでは、管理対象サーバーのソフトウェア構成が、サーバーにアタッチされているソフトウェアポリシーで指定された仕様に準拠しているかどうかをチェックします。

— **レポート**

SAでは、カスタマイズ可能なレポートが幅広く用意されていて、管理対象サーバーの状態に関するデータをさまざまなタイプのユーザー向けに提供できます。

変更内容のモデル化と検証を行ってから実際に管理対象サーバーを変更するので、変更時の安全性と一貫性を向上できます。また、管理対象サーバーで予定している変更を事前にテストできるので、ダウンタイムの短縮にもつながります。

SAの構成

SAの簡易インストールには、SAコア、コンポーネント、シングルサーバーでホストするOracleデータベースが含まれます。さらに高度なインストールでは、セカンダリコア (プライマリSAコアを補完してサーバー管理機能を強化) の追加、SAサテライト (SAコアに類似していますが規模は小さく機能も限られています。要件やリソースが小規模なデータセンターや支店で使用)、マルチマスターメッシュ (2つのSAコアが通信し、サーバーを共同管理) を追加できます。詳細については、第3章「SAアーキテクチャーの詳細」を参照してください。

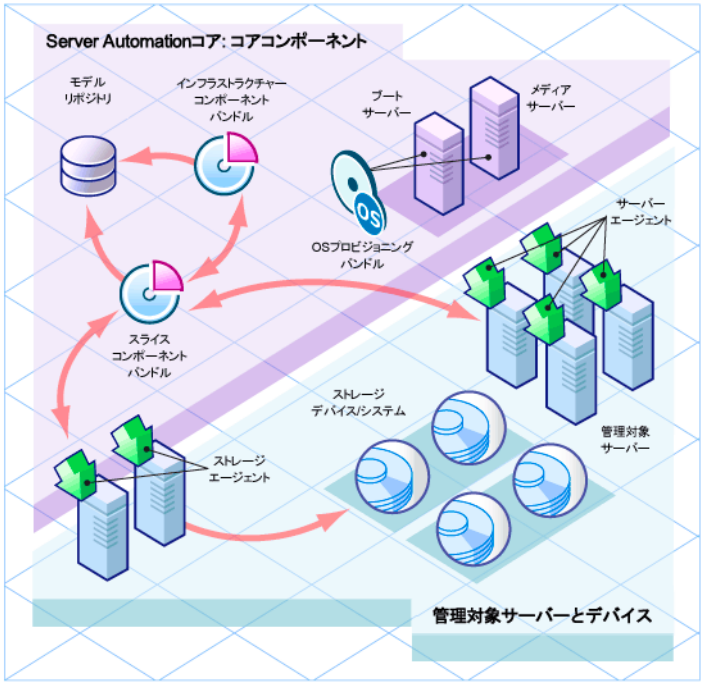
SAは、カスタマーインストールを8種類の構成でサポートします。この構成については、『SA Installation Guide』を参照してください。これ以外の構成では、カスタマーインストールではサポートされていないので、HPプロフェッショナルサービスが必要になります。

SAの簡易構成

SAは、サーバー管理機能を備えたさまざまなコンポーネントをインストールします。SAのインストールをカスタマイズする必要がない場合は、SAの単一ホストインストールを選択してください。また、パフォーマンス上の理由でSAコアコンポーネントを複数のサーバーに分散するなど、カスタマイズが必要な場合には、HPプロフェッショナルサービスまたは認定のHPコンサルタントをご依頼ください。

図1は、単一のデータセンター設備の場合の最もシンプルなSAインストールを示しています。この構成では、単一のネットワーク上にあるサーバーを管理する単一のホストに、すべてのSAコンポーネントをインストールします。

図1　　シンプルなSAインストール



Oracleデータベース

すべてのSAインストールにはSA用に構成したOracleデータベースが必要です。このデータベースはモデルリポジトリというSAコンポーネント (モデルリポジトリ (28ページ) を参照) が使用し、ネットワーク、ストレージデバイス、管理対象サーバー、管理対象サーバーにインストールされているオペレーティングシステムとアプリケーションに関する情報を保存します。このデータベースは、SAのインストール時に提供されます。または、SA用に構成した既存のOracleインストールも使用可能です (詳細については、『SA Installation Guide』の「Appendix A: Oracle Setup for the Model Repository」を参照してください)。

SA機能へのアクセス

SA機能には、次の2つの方法でアクセスできます。

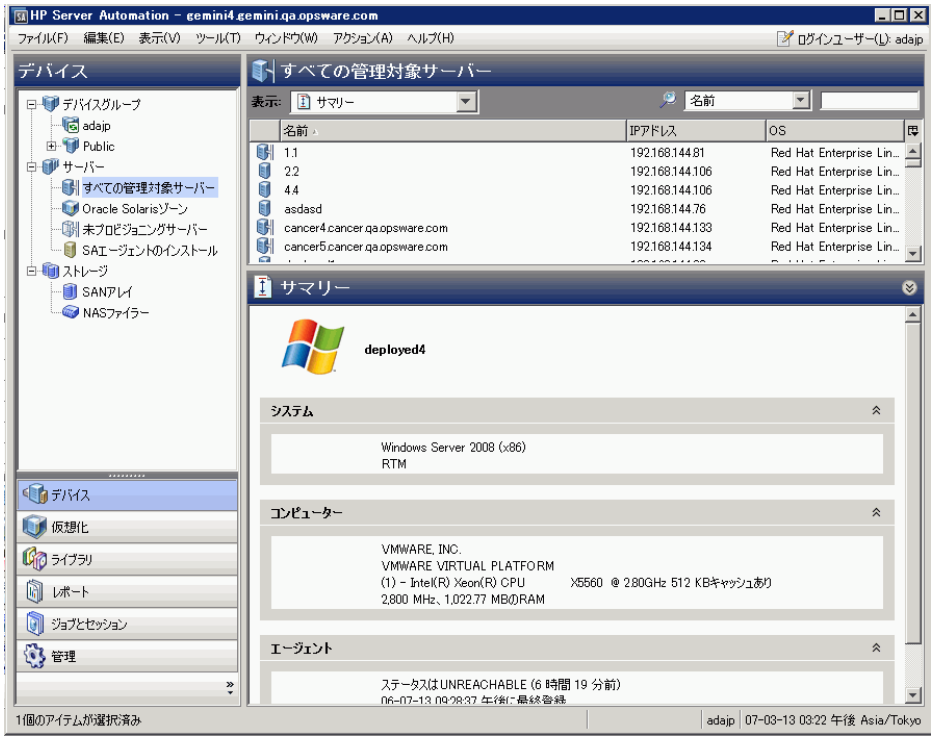
SAクライアント

SAクライアントはWindowsアプリケーションであり、SAの後にインストールします。SAへのインタフェースとして機能します。

SAクライアントをインストールするには、SA Launcherのダウンロードが必要です。コアへのログインページを開き、[Download Hewlett-Packard Launcher] リンク (『SAユーザーガイド: Server Automation』を参照) をクリックしてください。

図2は、SAクライアントのメイン画面です。SAクライアントの詳細については、『SAユーザーガイド: Server Automation』を参照してください。

図2　　SAクライアントのメイン画面



SA Webクライアント

SA Webクライアントは、推奨されていません。いくつかのSA機能は今でもSA Webクライアントによって提供されていますが、可能であればSAクライアントを使用してください。

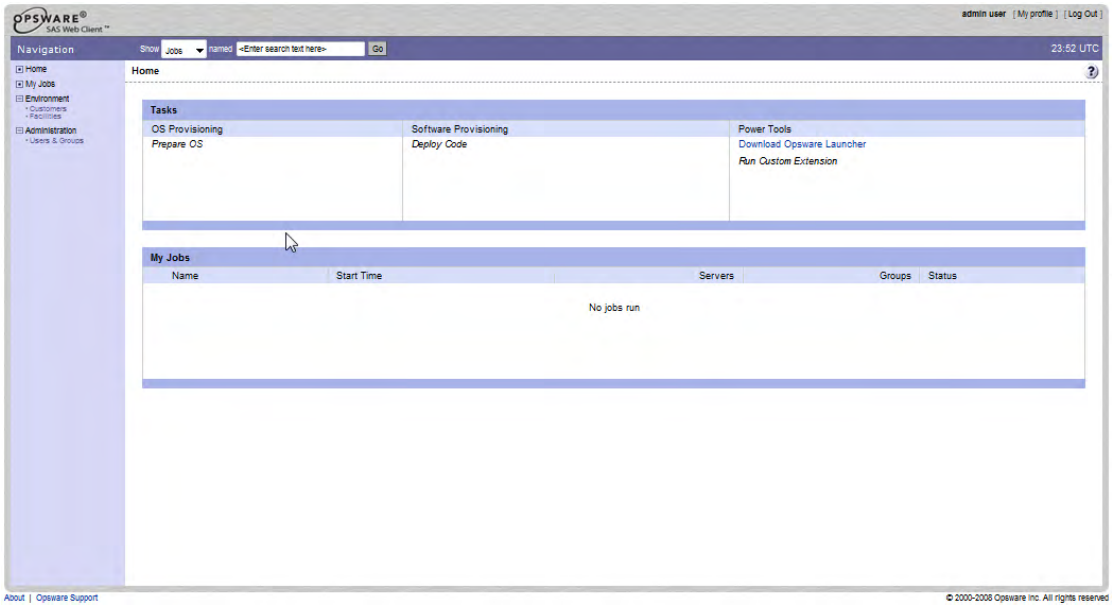
SA Web クライアントは、Web ベースの SA とのユーザーインタフェースであり、サーバー管理に使用します。ブラウザーでSA Webクライアントを起動する手順は、『SAユーザーガイド: Server Automation』を参照してください。SA Webクライアントが起動したら、[タスク] ペインでSAクライアント Launcherの実行可能ファイルをダウンロードし、インストールします。

SA Webクライアントには次の項目があります。

- **Tasks**
  - SAクライアントの実行可能ファイルのダウンロード
  - 分散スクリプトの実行
  - カスタム拡張の実行
- **My Jobs**: これまでに実行したジョブ、現在実行中のジョブ、実行予定のジョブの詳細情報
- **My Customers**: SAコアに関連付けられているカスタマーの情報。

図3は、SA Webクライアントのホームページを示します。

図3　　SA Webクライアントのホームページ



サンプルのユースケースとチュートリアル

第2章「SA機能の概要」では、SA機能の使用方法の概要について説明します。また、『SA Getting Started』ガイドでは対話型のチュートリアルが提供されており、オペレーティングシステムのサーバーへのインストール、ソフトウェアポリシーの作成、Windows/Solarisのパッチ適用などの手順を学習できます。SAクライアントにも対話型のチュートリアルが提供されており、オンラインヘルプからアクセスできます。

第2章 SA機能の概要

SAは、ミスが発生しやすい手動のアドホックなデータセンタープロセスを自動化します。たとえばOSプロビジョニングでは、サーバーのタイプごとに標準を設定し、サーバープロビジョニングを自動化します。これによって、時間が節約できるだけでなく、一貫性のあるオペレーティングシステム環境を構築できます。

パッチポリシーでは、IT環境内の管理対象サーバーで稼働するサポート対象オペレーティングシステムにおいて、パッチのインストールと管理を実行できます。

コンプライアンスでは、管理対象サーバーにコンプライアンス違反がないかを把握できます。非コンプライアンスサーバーが検出されたら、作成したポリシーに基づいて修復し、準拠した状態に戻します。

SAでは、次の機能を提供しています。

- オペレーティングシステムのプロビジョニング
- アプリケーションデプロイメント
- スクリプト実行
- エージェントレスサーバーの検出とエージェントのインストール
- デバイスエクスプローラー
- 仮想化の管理
- Service Automation Visualizer (SAV)
- Storage Visibility and Automation
- 監査と修復
- SAクライアントでのコンプライアンス
- レポート
- ソフトウェア管理
- Windowsパッチ管理
- HP-UXパッチ管理
- UNIXパッチ管理
- SolarisおよびSolaris 11のパッチ管理
- Ubuntuパッチ管理
- アプリケーション構成管理
- Global Shell

SAは、クロスプラットフォームをサポートし、新規と既存のデータセンター環境の自動化に対応します。

オペレーティングシステムのプロビジョニング

SAのOSプロビジョニングでは、ベアメタルサーバーと仮想サーバーに対して事前構成済みのオペレーティングシステムベースラインのインストール (またはプロビジョニング) を一貫した方法で迅速に実行し、手動による操作を最小限に抑えることができます。ベアメタルサーバーと仮想サーバーでのOSプロビジョニングは、サーバーを運用環境に移行するプロセス全体の中で重要な部分です。

OSプロビジョニングにより、ファシリティ内の各サーバーに、標準として定められたデフォルトのオペレーティングシステム構成を適用することができます。OSプロビジョニングの詳細については、『SA ユーザーガイド: プロビジョニング』を参照してください。

SAのOSプロビジョニングには、次のような利点があります。

- **他のSA機能との統合**

  SAのOSプロビジョニングは、パッチ管理、ソフトウェア管理、分散スクリプト実行といったSAの自動化機能と統合されているので、ITグループ間でシームレスな受け渡しが可能になります。SAを使用することによって、すべてのITグループが環境の現状を理解した上で連携できるので、高品質のオペレーションと信頼性の高い変更管理を実現する上で大きな効果を発揮します。

- **イメージの再適用なしでサーバーベースラインを更新**

  他のOSプロビジョニングソリューションとは異なり、SAでプロビジョニングを行ったシステムは、プロビジョニング後も簡単に変更でき、新しい要件に適応させることができます。これを可能にしているのが、テンプレートの使用と、インストールベースでプロビジョニングを行うアプローチです。

- **さまざまな環境に対応できる柔軟なアーキテクチャー**

  SAのOSプロビジョニングでは、さまざまなタイプのサーバー、ネットワーク、セキュリティアーキテクチャー、オペレーションプロセスがサポートされます。SAは、CD (Linuxプロビジョニング) やネットワークブート環境 (DHCPと非DHCPの両方の環境) で問題なく動作し、スケジュールされたワークフローまたはオンデマンドのワークフロー、幅広いハードウェアモデルをサポートします。このように優れた柔軟性を備えているので、ユーザー組織のニーズに合わせたオペレーティングシステムのプロビジョニングが可能になります。

OSプロビジョニングは、SAクライアントとSA Webクライアントのいずれからも実行できます。SAは、包括的なサーバーベースラインのプロビジョニングプロセス全体を自動化します。これは次のタスクで構成されます。

- OS インストールプロファイルを使用して、OS をインストールできるようにハードウェアを準備します (OSシーケンスのみで必要)。
- オペレーティングシステムインストールの前後に実行するタスクを定義する OS ビルド計画を作成します。OSビルド計画は、OSシーケンスの代わりに使用すると便利です。
- インストール中にサーバーで実行するタスクを定義する OS シーケンスを作成します。OS シーケンスでは、アプリケーション、パッチ、修復の各ポリシーを定義できます。ただし、OSシーケンスよりも柔軟性の高いOSビルド計画の使用をお勧めします。
- OSビルド計画またはOSシーケンスを使用して、基本オペレーティングシステムとデフォルトのOS構成をインストールします。
- 最新のOSパッチセットを適用します。実際の内容は、サーバーで実行するアプリケーションによって異なります。
- root パスワードなどのシステム構成を行うインストール前スクリプトまたはインストール後スクリプトを実行します。
- システムエージェントとユーティリティ (SSH、PC Anywhere、バックアップエージェント、監視エージェント、ウイルス対策ソフトウェアなど) をインストールします。
- Java仮想マシンなど、広い範囲で共有するシステムソフトウェアをインストールします。

SA OSプロビジョニングのサポート対象:

- Windows、Solaris、Linux
- ネットワークベースまたはCD/DVDベースのインストール
- データセンターのスタッフとシステム管理者の作業分担
- モデルベースのアプローチにより、多数のシステムにインストール可能な標準ビルドをSAで作成

OSプロビジョニングは、オペレーティングシステムベンダー独自のインストールテクノロジーを統合します。

- Windowsセットアップ作業の応答ファイル: `unattend.txt`、`unattend.xml`、`sysprep.inf`
- Red Hat Kickstart
- SuSE YaST (Yet another Setup Tool)
- Solaris Jumpstart
- WINPE/WIN-BCOM/UNDI

オペレーティングシステムのプロビジョニングは、次のサーバーで実行できます。

- SAのエージェントレスサーバープールに含まれ、オペレーティングシステムがインストールされていないサーバー (ベアメタルサーバー)
- 仮想サーバー
- SAの非管理対象サーバープールに含まれ、オペレーティングシステムがインストール済みのサーバー
- SA の管理対象サーバープールに含まれ、オペレーティングシステムがインストール済みのサーバー (再プロビジョニング)

アプリケーションデプロイメント

アプリケーションデプロイメントでは、データセンター内のターゲットサーバーで、カスタムソフトウェアアプリケーションの作成、テスト、デプロイメントを行います。たとえば、テストを行う目的で、アプリケーションを開発チームから品質保証チームに移動します。テストが完了したアプリケーションは、運用準備、ステージング、さらに運用開始など各フェーズへと移動します。アプリケーションデプロイメントツールでは、単一のアクセスポイントから、すべてのユーザーがそれぞれの役割に応じて関連データを表示または入力できるので、アプリケーションのデプロイメントに伴う複雑なコミュニケーションを簡略化できます。

アプリケーションデプロイメントには次のような機能があります。

- コード、スクリプト、構成ファイル、層 (アプリケーションサーバー、Web サーバー、データベースなど) といったアプリケーションコンポーネントをモデル化します。
- アプリケーションの複数のリリースとバージョンを管理します。
- ターゲットサーバーでアプリケーションのデプロイ、ロールバック、アンデプロイを行います。
- アプリケーションで必要になる層を実行するターゲットサーバーをモデル化します。このターゲットサーバーは、Server Automationで管理します。
- ソフトウェアアプリケーション開発者、品質保証およびテスト担当者、システム管理者、その他オペレーションの担当者が、相互に明確で簡潔な方法でコミュニケーションを図る手段を提供します。
- アプリケーション開発、QA、運用準備、ステージング、運用開始というライフサイクルをモデル化し、実装します。ユーザーのエンタープライズライフサイクルに合わせたカスタマイズが可能です。

詳細については、『SA User Guide: Application Deployment Manager』を参照してください。

スクリプト実行

SAのスクリプト実行では、SAで管理するサーバーファーム全体で、アドホックスクリプトや保存済みスクリプトを共有および実行できます。

手動ではなくSAを使用してスクリプトを実行する方法には、次のような利点があります。

- 多数のUNIXまたはWindowsサーバーでスクリプトを並列実行することにより、時間を節約できるだけでなく、一貫性を維持できます。
- 役割ベースのアクセス制御を適用することで、承認した管理者のみに、アクセス権を持つホストでのスクリプト実行を許可します。
- プライベートライブラリとパブリックライブラリにスクリプトを保存し、スクリプトのアクセス制御を行います。
- スクリプト出力の表示とダウンロードを行います。サーバーごとのレポート、またはすべてのサーバーの出力を1箇所に集約したレポートを作成します。
- スクリプトの一括カスタマイズが可能です。管理者は、SAに保存されているサーバーの環境と状態に関する情報にアクセスできます。これは、適切なサーバーで適切なスクリプトを実行する上で非常に重要な機能です。
- 包括的な監査証跡を作成し、各スクリプトの実行者と実行日時を記録します。

スクリプト実行はSAの統合された機能であり、スタンドアロンのスクリプト実行ツールに比べて、次のような利点があります。

- システムの状態や構成情報をベースに、スクリプト実行をカスタマイズできます。SAには、サーバーを所有するカスタマーやビジネス、サーバーがステージングサーバーか運用サーバーかの区別、サーバーが設置されているファシリティ、カスタマイズした名前と値のペアなどさまざまな情報が保存されているので、これを参照またはアクセスすることでスクリプトをカスタマイズします。
- セキュリティを損なわない方法でスクリプトを共有できます。SAでは、スクリプト実行を許可するユーザーと対象サーバーのアクセス制御が厳格に実施され、スクリプト実行の監査証跡が作成されるので、セキュリティを損なわずにスクリプトを共有できます。

エージェントレスサーバーの検出とエージェントのインストール

エージェントレスサーバーの検出とエージェントのインストールでは、ファシリティ内にある多数のサーバーにサーバーエージェントをデプロイし、SAで管理することができます。

次のタスクを実行できます。

- ネットワークでエージェントレスサーバーをスキャンします。
- SAエージェントをインストールするサーバーを選択します。
- 通信ツールを選択し、ユーザーとパスワードを提供します。
- エージェントのインストールオプションを選択し、エージェントをデプロイします。

デバイスエクスプローラー

デバイスエクスプローラーでは、管理対象環境で稼働するサーバーの情報が表示されます。

サーバーエクスプローラーでは、次のタスクを実行できます。

- サーバースナップショットの作成、サーバー監査の実行、アプリケーション構成の監査、パッケージの作成、リモートターミナルセッションをリモートサーバーで開く、などを実行します。

— サーバーのファイルシステム、レジストリ、ハードウェアインベントリ、ソフトウェアとパッチのリスト、サービスを参照します。

— SAの情報 (プロパティ、構成可能なアプリケーション、サーバー履歴など) を参照します。

グループブラウザーでは、次のタスクを実行できます。

— システム情報の監査、サーバースナップショットの取得、アプリケーションの構成を行います。

— グループ メンバー (サーバーグループとその他グループ) の表示とアクセスを行います。

— グループのサマリー情報と履歴情報を表示します。

仮想化の管理

HPでサポートする仮想化ベンダーとクラウドコンピューティングの統合ソリューションは、仮想化サービスと呼ばれます。

仮想化ベンダーは、仮想化環境内の複数のハイパーバイザーと VM を管理します。HP では、VMware vCenter サーバーやMicrosoft System Center Virtual Machine Manager (SCVMM) との統合をサポートしています。

OpenStackなどのクラウドコンピューティングソリューションでは、サービスとしてのインフラストラクチャ (IaaS) が提供されています。HPでは、OpenStackとの統合を制限付きでサポートしています。

HP Server Automationで仮想化を管理すると、次のような利点があります。

- データセンター、すべての物理マシンと仮想マシン (VM) を可視化します。
- 法規制や社内ポリシーすべてにおいてコンプライアンスを確保します。
- 仮想環境全体を管理することにより、VMの無秩序な増加を防止し、短時間で問題を解決します。

Service Automation Visualizer (SAV)

Service Automation Visualizer (SAV) は、IT環境内に分散したビジネスアプリケーションについて、オペレーションアーキテクチャーと動作に関する情報提供と管理を効率的に行います。分散ビジネスアプリケーションは、多くのサーバーで実行されるサービス、ネットワーク、ストレージデバイスを含む複雑な構成なので、相互の関連性、パフォーマンス低下の原因、トラブルシューティングと問題解決の方法、環境の変更がもたらす結果を把握することはますます難しくなっています。

SAVでは、このような情報を物理的な側面と論理的な側面からグラフィック表示します。

Storage Visibility and Automation

Storage Visibility and Automation は、ストレージサプライチェーン全体の表示と管理をエンドツーエンドに実行することによってストレージ管理を行います。Storage Visibility and Automation は、アプリケーションストレージ、依存関係と可視化、ストレージの監査、ストレージの容量と利用率のトレンド分析、スクリプト作成と自動化などのコスト削減ツールを提供することによって、サーバー管理者が日々行う作業をサポートします。詳細については、『Storage Visibility and Automationユーザーガイド』を参照してください。

監査と修復

監査と修復では、IT環境内でチェック対象のオブジェクト、チェックを行う場所とタイミングを指定できます。

- 監査ポリシーでは、チェック対象 (ファイル、ディレクトリ、構成値など) を定義します。
- 監査では、チェック対象となる場所 (サーバー、サーバーグループなど) を定義します。
- 監査スケジュールでは、チェックを行うタイミング (特定の日時、反復実行など) を定義します。

これらの機能を使用することによって、管理対象サーバー環境でコンプライアンスを確保し、サーバーのコンプライアンス状態を維持する方法を理解できます。SAでは、ファシリティ内のサーバーを標準ポリシーに準拠した状態にする方法として、サーバー構成ポリシーを使用します。非コンプライアンス状態 (想定通りに構成されていない状態) として検出されたサーバーは、修復によって、組織で規定されている標準に準拠した状態にすることが可能です。

SAクライアントでは、動作中のサーバーまたはサーバースナップショット、ユーザー指定の値、事前定義された監査ポリシーをベースに、サーバー構成値の監査を実行します。また、サーバー構成スナップショットを使ってシステムの現在の状態を取得し、他のサーバーと比較することも可能です。

監査ポリシーでは、会社全体または業界共通のコンプライアンスおよびセキュリティ標準を定義し、監査やスナップショット仕様などの監査ポリシーで使用できます。監査やスナップショット仕様で定義した監査ポリシーを参照すれば、組織内の最新のコンプライアンス定義に適応できているかどうかを確認できます。

監査と修復では、次のタスクを実行できます。

- サーバーまたはスナップショットと評価基準となるサーバーまたはスナップショットとの比較
- 反復使用できる監査の作成
- 組織に適用するコンプライアンス標準およびセキュリティ標準を定義する監査ポリシーを作成
- 個々のサーバーまたは動的なサーバーグループに監査を関連付ける
- 複数のレベル (ファイル、ディレクトリ、パッチ、レジストリキー、パッケージなど) で問題を修復

SAクライアントでのコンプライアンス

SAクライアントのコンプライアンスビューでは、ファシリティ内にあるすべてのサーバーとサーバーグループの全体的なコンプライアンスレベルを確認できます。一般的にはコンプライアンスダッシュボードと呼ばれるこのビューから、非コンプライアンス状態のサーバーを修復することができます。コンプライアンスを表示する対象として、個々のサーバー、複数のサーバー、サーバーグループ、すべてのSA管理対象サーバーを選択できます。

コンプライアンスダッシュボードには、サーバーまたはサーバーグループの監査、監査ポリシー、ソフトウェアポリシー、パッチポリシー、アプリケーション構成に対するすべてのコンプライアンスステータスの結果が表示されます。サーバーのコンプライアンスステータスは、コンプライアンスポリシーを基準に判定されます。コンプライアンスポリシーではサーバー構成の設定や値が一意に定義されており、これに基づいてIT環境が想定通りに構成されているかどうかが確認されます。

コンプライアンスポリシーの作成と定義は、一般的にポリシー設定の担当者が行います。環境によっては、システム管理者がアドホックポリシーを作成する場合もあります。ポリシー設定担当者は、作成したコンプライアンスポリシーをサーバーにアタッチします。これによって、サーバーが組織の標準とポリシーに準拠しているかどうかを確認できます。

たとえば、ポリシー設定の担当者は、ソフトウェアポリシーを作成し、サーバー上にインストールしなくてはならないパッチとパッケージの標準セットを定義します。また、サーバーでの特定のアプリケーションファイルの構成方法も定義できます。サーバーまたはサーバーグループの構成が、ポリシー設定担当者がコンプライアンスポリシーで定義したルールと一致した場合、コンプライアンス状態であるとみなされます。

コンプライアンスダッシュボードでは、サーバーにインストールされているソフトウェア、パッケージ、パッチ、構成ファイルの実際の設定が、ソフトウェアポリシーで定義した構成と一致しているかどうかを確認できます。コンプライアンスビューでは、サーバーグループのコンプライアンスステータスを、グループのすべてのメンバーとサブグループのメンバーごとに表示できます。また、非コンプライアンス状態のサーバーとサーバーグループを検出し、問題を修復できます。

レポート

SAのレポートでは、環境内の管理対象サーバー、ネットワークデバイス、ソフトウェア、パッチ、カスタマー、ファシリティ、オペレーティングシステム、コンプライアンスポリシー、ユーザーとセキュリティに関する包括的な情報がリアルタイムで提供されます。レポートはグラフと表の形式で提示され、ポリシーや監査などのレポート内のオブジェクトに対して適切なアクションを実行できるようになっています。また、組織で使用しやすいファイル形式(`.html`と`.xls`)でローカルファイルシステムにエクスポートもできます。

ソフトウェア管理

ソフトウェアポリシーを使用してソフトウェアをモデル化し、サーバーでのソフトウェアのデプロイとアプリケーションの構成を1つのステップで自動化する強力な機能があります。さらに、ソフトウェアリソースをフォルダー構造にまとめ、セキュリティに関するアクセス権を定義することもできます。また、サーバーのコンプライアンスステータスを検証し、非コンプライアンスサーバーを修復する機能もあります。

ソフトウェア管理では、次の機能を提供しています。

- ソフトウェアの組織構造を作成
- フォルダーでのセキュリティ境界を定義
- 組織内にあるIT環境の管理に適用するモデルベースのアプローチを定義
- ユーザーグループ間でソフトウェアリソースを共有
- アプリケーションのデプロイと構成を同時実行
- 1つのサーバーに複数のアプリケーションインスタンスをデプロイ
- ソフトウェアデプロイメントプロセスを確立
- ソフトウェアポリシーに基づいてサーバーのコンプライアンスステータスを検証
- レポートを作成
- ソフトウェアリソースとサーバーを包括的に検索

詳細については、『SA ユーザーガイド：ソフトウェア管理』のソフトウェア管理のクイックスタートを参照してください。

Windowsパッチ管理

Windowsパッチ管理では、Microsoft® Windowsパッチの確認、インストール、削除によって、組織内にある管理対象サーバーのセキュリティを確保します。Windowsオペレーティングシステムについて、セキュリティの脆弱性に対するパッチを確認し、インストールできます。

詳細については、『SA Support and Compatibility Matrix』を参照してください。

Windowsではセキュリティの脅威に対するパッチが頻繁にリリースされるので、システムをリスクにさらさないようにするには迅速にパッチを適用する必要があります。ただし、パッチを誤って適用すると、パフォーマンスの低下や重大なエラーなど深刻な問題が発生する原因になるので注意が必要です。

パッチ管理では、新しく検出された脅威に迅速対応できるだけでなく、パッチインストールの厳格なテストと標準化をサポートします。さらに、パッチが原因で問題が発生した場合には、テストと承認の後であっても、Windowsパッチ管理で安全かつ標準化された方法でパッチをアンインストールできます。

詳細については、『SA ユーザーガイド：サーバーのパッチ適用』のパッチ管理のクイックスタートを参照してください。

HP-UXパッチ管理

SAでは、次の機能によってHP-UXパッチ管理を自動化します。

- モデルベースのアプローチで HP-UX サーバーを管理する HP-UX ソフトウェアポリシーを定義します。Server Automationでは、HP-UXソフトウェアポリシーを使用して、IT環境のモデルを作成できます。これらのソフトウェアポリシーでは、管理対象サーバーにインストール可能なパッチとスクリプトを指定します。
- HP-UXパッチとパッチバンドルを管理対象サーバーにインストールします。
- パッチインストールプロセスを確立します。
- パッチ管理の各ステージ (分析、ダウロード、インストール) のスケジュールを設定します。また、各ステージごとに電子メール通知を設定し、ジョブにチケットIDを関連付けることもできます。
- ソフトウェアポリシーに基づいて、サーバーのコンプライアンスステータスを検証します。
- コンプライアンスビューで、サーバーがソフトウェアポリシーに基づいて構成されているかを確認し、非コンプライアンスサーバーがあれば修復します。
- ソフトウェアリソースとサーバーを検索します。
- SAライブラリでは、強力かつ柔軟な検索条件 (可用性、アーキテクチャー、オペレーティングシステム、再起動オプション、バージョンなど) を使用して、HP-UXパッケージ、パッチ、ソフトウェアポリシーを検索します。HP-UX ソフトウェアポリシーは、名前、フォルダー名、可用性、オペレーティングシステムで検索することも可能です。
- パッチインストールのプレビューでは、パッチの依存関係とパッチの適用性分析が表示されます。

詳細については、『SA ユーザーガイド：サーバーのパッチ適用』のパッチ管理のクイックスタートを参照してください。

SolarisおよびSolaris 11のパッチ管理

Server Automation パッチ管理では、Solaris パッチの確認、インストール、削除によって、組織内にある管理対象サーバーのセキュリティを確保します。

Server AutomationのSolarisパッチ管理は、パッチポリシーを適用することによって、Solarisパッチとパッチクラスターのインストールとアンインストールを自動化します。さらに、ポリシー内のパッチ間の依存関係、優先度、適用可能性を分析し、サーバーへのインストール順序を示す最新のパッチリストを表示します。この機能により、サーバーのコンプライアンスステータスが検証できます。非コンプライアンスサーバーが検出された場合は修復し、SolarisパッチをSAに自動ダウンロードしてパッチポリシーに組み込むことができます。

SAでは、次の機能によってSolarisでのパッチ適用を自動化します。

- 管理対象サーバーで必要なパッチを特定します。
- Solarisパッチポリシーを作成します。
- Solaris パッチ、パッチクラスター、パッチバンドルをダウンロードし、さらにそれらと関連ベンダー情報をSAライブラリに保存します。

- Solarisパッチが依存するパッチをすべて解決します。
- Solarisパッチとパッチクラスターを管理対象サーバーにインストールします。
- Solarisパッチをシングルユーザーモードでインストールします。
- Oracle Solarisゾーンごとにパッチをインストールします。
- パッチインストールプロセスを確立します。
- パッチポリシーに基づいて、サーバーのコンプライアンスステータスを検証します。
- ソフトウェアリソースとサーバーを検索します。

詳細については、『SA ユーザーガイド : サーバーのパッチ適用』のパッチ管理のクイックスタートを参照してください。

Ubuntuパッチ管理

HP Server Automation (SA) のUbuntuパッチ管理では、Ubuntu Debianパッケージ更新の確認、インストール、削除によって、組織内にある管理対象サーバーのセキュリティを確保します。SA でサポートされる管理対象サーバープラットフォームのセキュリティ脆弱性に対して、対応する Ubuntu パッケージを確認してインストールすることができます。

SA ではパッチ管理の主要な機能が自動化されていますが、Ubuntu パッケージのインストール方法やインストール条件は、細かく制御することができます。パッチ適用プロセスを自動化することで、パッチ適用に伴うダウンタイムを短縮できます。また、SA では、パッチアクティビティのスケジュールを設定することで、ピーク以外の時間帯にパッチを適用することができます。

ベストプラクティス: SA の Ubuntu パッチ適用を使用して、バイナリパッケージをインポートする前にメタデータをインポートできます。ダウンロードしたメタデータのみを使用して、Ubuntu スキャナーを実行し、サーバーの脆弱性を特定できます。その後、Ubuntuパッケージインポーターを実行して、管理対象サーバーに必要なパッケージのみをインポートできます。この方法により、ストレージ容量と、スキャンおよび修復プロセス時間を節約できます。

Ubuntu パッチ管理のドキュメントには、Ubuntu メタデータおよびパッケージのインポート方法、脆弱性のスキャン、パッチポリシーを使用したUbuntuパッケージ更新のインストールに関する情報が記載されています。

SAでは、次のような機能や特徴を利用して、Ubuntuパッチ適用を自動化しています。

- **セントラルリポジトリ**: パッケージがそれぞれの標準形式で保存され、整理されます
- **データベース**: これまでに適用したすべてのパッケージの情報を保存します
- **動的パッチポリシー** : ベンダーの最新メタデータに基づいてプラットフォームの脆弱性を分析します。
- **高度な検索機能**: パッケージ更新が必要なサーバーを識別できます
- **監査機能**: 重要なパッケージ更新のデプロイメントをトラッキングします

詳細については、『SA ユーザーガイド : サーバーのパッチ適用』のパッチ管理のクイックスタートを参照してください。

UNIXパッチ管理

UNIX パッチ管理では、パッチの確認、インストール、削除によって、組織内にある管理対象サーバーのセキュリティを確保します。SAクライアントは、AIXオペレーティングシステム環境に存在するセキュリティの脆弱性に対するパッチを特定して、インストールできます。

SAは、新しく検出された脅威に迅速対応できるだけでなく、パッチインストールの厳格なテストと標準化をサポートします。さらに、パッチが原因で問題が発生した場合には、テストと承認の後であっても、安全かつ標準化された方法でパッチをアンインストールできます。

SAは、SAライブラリにパッチ情報を保存します。これには、管理対象サーバー、サーバー上にインストールされているパッチとソフトウェア、インストール可能なソフトウェアとパッチに関する詳細な情報が含まれます。このデータを元に新しく検出された脅威の重大度を判定し、パッチをインストールした場合のメリットとダウンタイムコストを比較して、テスト要件を特定します。

パッチの適用手順を自動化することで、パッチ適用に伴うダウンタイムを短縮できます。また、パッチアクティビティのスケジュールを設定することで、ピーク以外の時間帯にパッチを適用することができます。

UNIXパッチ管理では、次の機能が提供されているため、オペレーティングシステムごとのパッチの参照、パッチのダウンロードとインストールのスケジュール設定、電子メール通知の設定、パッチインストールのプレビュー、ソフトウェアポリシーと修復によるパッチのインストールとアンインストール、再利用可能なファイル形式へのパッチ情報のエクスポートなどを実行できます。

- パッチの保存先であり、各形式で編成されているSAライブラリ
- これまでに適用したパッチの情報が格納されたデータベース
- パッチインストールの前後に実行できるカスタマイズスクリプト
- パッチの適用が必要なサーバーを特定できる高度な検索機能
- セキュリティ担当者が重要なパッチのデプロイメントを追跡できる監査機能

詳細については、『SA ユーザーガイド : サーバーのパッチ適用』のパッチ管理のクイックスタートを参照してください。

アプリケーション構成管理

アプリケーション構成管理 (ACM) は、テンプレートを作成することによって、サーバーアプリケーションに関連付けられているアプリケーション構成の変更と管理を行います。このような構成の管理、更新、変更を一元的に行うことで、ファシリティ内のアプリケーションの構成を正確で一貫性のある状態に維持できます。

ACMでは、次のタスクを実行できます。

- ファイルとオブジェクト (Windowsレジストリ、IISメタベース、WebSphere、COM+など) に基づいて構成を管理します。
- 構成変更を適用する前に、変更前にプレビューします。
- 構成変更を編集し、個々のサーバーまたはサーバーグループにプッシュします。
- SAデータモデルの情報を使用して、構成値を設定します。
- 構成テンプレートを作成することにより、任意のアプリケーションの構成を管理します。
- サーバーのアプリケーション構成を監査し、サーバー上にテンプレートで指定した値と一致しない構成ファイルがないか確認します。

詳細については、『SA ユーザーガイド : アプリケーション構成』のアプリケーション構成のクイックスタートを参照してください。

Global Shell

SA Global Shell では、コマンドラインインタフェースからサーバーを管理します。次のタスクをリモート実行できます。

- 管理対象サーバーで繰り返し行う管理タスクを実行します。
- 管理対象サーバーで発生した問題のトラブルシューティング、特定、修復を行います。

Global Shell では、SA 内のサーバー管理にファイルシステムとコマンドラインインタフェースを使用します。このファイルシステムはSA Global File System (OGFS) と呼ばれます。OGFS内にあるすべてのタイプのオブジェクト (サーバー、カスタマー、ファシリティなど) はファイルシステムのディレクトリ構造で表示されます。

また、管理対象サーバー上にあるファイルシステム、Windowsレジストリ、Windowsサービスオブジェクトに対するユーザーアクセス権を管理することもできます。

第3章 SAアーキテクチャーの詳細

ここでは、SAコアのレイアウトのカスタマイズ、マルチマスターメッシュの作成、データベースのリモートインストールなどを予定しているユーザーを対象に、SA アーキテクチャーについてさらに詳しく説明します。SAコアとコアコンポーネントの詳細と、コア、サーバーエージェント、サテライト間の関係についても説明します。

SAコア

SAコアは、コアコンポーネントのグループであり、連携して動作します。コアによって、ネットワーク上でサーバーを検出し、これを管理対象サーバープールに追加した後、プロビジョニング、構成、パッチの適用、監視、監査、管理などの作業をSAクライアントインタフェースから一元的に実行できます。SAクライアントでは、1つのインタフェースからSAのすべての情報と管理機能を操作できます。

コアコンポーネントのインストール先となるサーバーは、コアサーバーと呼ばれます。コアコンポーネントは、複数のホストに分散されている場合でも、1つのSAコアの一部として認識されます。

コアコンポーネントは、1つのホストにインストールまたは複数のホストに分散できますが、一般的なSA インストールではコアコンポーネントバンドルが使用されます。バンドルとは、パフォーマンスと管理効率の向上を目的に、いくつかのコンポーネントをまとめて同じサーバーにインストールする方法です。コンポーネントバンドルの詳細については、SAコアコンポーネントのバンドル (27ページ) を参照してください。

SAでは、いくつかのサーバー管理アクティビティとの通信と管理の目的で、各管理対象サーバーにサーバーエージェントがインストールされます。これにより、管理対象サーバーとの通信を、SAコアコンポーネントの一部であるゲートウェイ経由で行うことができます。またサーバーエージェントは、SAクライアントまたはSA Webクライアントからユーザーが入力した内容に基づいて、管理対象サーバーでアクションを実行します。

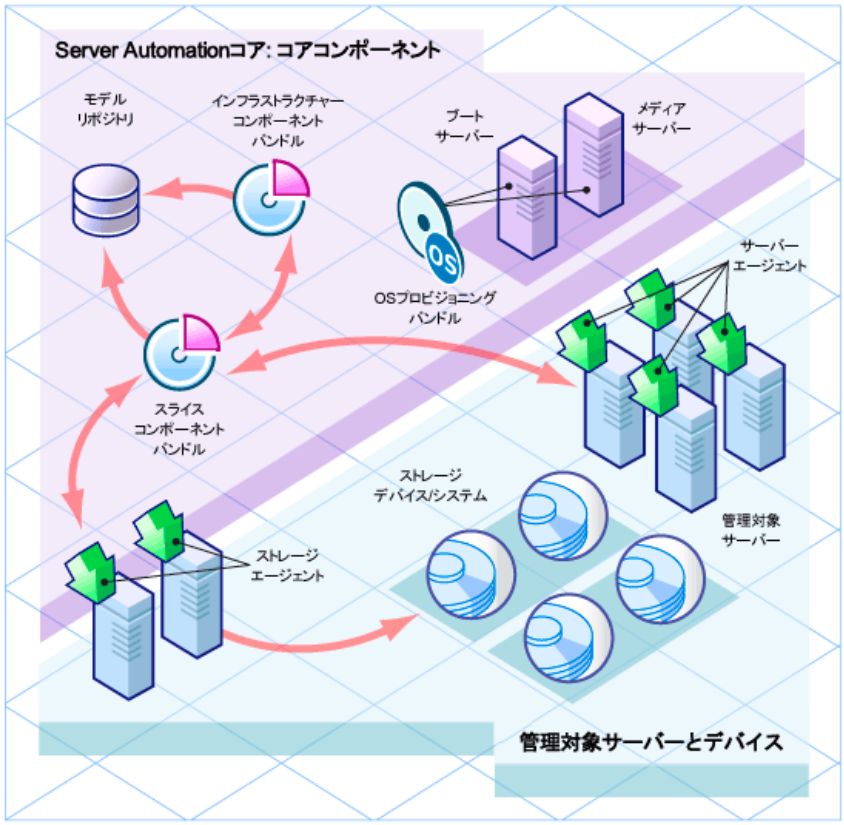
シンプルな単一ホストのインストール

図4は、SAコアを1つのホストにインストールした例を簡略化したものです。すべての管理対象サーバーが1つのファシリティ内にあり、このコアが一般的にマルチマスターメッシュの第1コアになります。多くの場合、各ファシリティで複数のコアをインストールします。SAのトポロジ (34ページ) を参照してください。

図では、単一のコアサーバーがSAコアコンポーネントをすべてホストしています。SAは、ネットワーク上にあるすべてのサーバーと、各種タスク (監視、監査、プロビジョニング、管理など) を実行するコンポーネントについて、場所と構成に関する情報の検出と保存を行います。

SAコアコンポーネントには、モデルリポジトリ、インフラストラクチャーコンポーネントバンドル、スライスコンポーネントバンドル、OSプロビジョニングコンポーネントバンドルがあります。管理対象サーバーについて見ると、すべての管理対象サーバーとストレージデバイスにはSAエージェントがインストールされます。このエージェントはゲートウェイ経由でコアと通信し、コア側でユーザーが指示したタスク (OSプロビジョニング、監査とレポートの実行など) を実行します。

図4　SAコアとエージェント



SA サーバーエージェント

SA サーバーエージェントは、SA で管理するすべてのサーバーにインストールされる高機能ソフトウェアです。エージェントレスサーバーにエージェントをインストールすると、エージェントはサーバーをSAに登録し、これによってサーバーは管理対象サーバープールに追加されます。またSAエージェントは、ユーザーが入力したコマンドをコアから受信し、エージェントがインストールされているサーバーで適切なアクションを実行します。このアクションには、ソフトウェアのインストールと削除、ソフトウェアとハードウェアの構成、サーバーステータスのレポート作成、監査などがあります。

SAエージェントは、次の方法でサーバーにインストールできます。

- SAエージェントデプロイメントツール (ADT) を使用して、SAサーバーエージェントがインストールされていないサーバー (エージェントレスサーバー) をネットワーク上で検出し、エージェントをインストールします。ADTの詳細については、『SAユーザーガイド: Server Automation』を参照してください。
- SAのOSプロビジョニングを使用して、ベアボーンサーバーでオペレーティングシステムのプロビジョニングを実行します。これにより、SAサーバーエージェントはオペレーティングシステムと一緒にインストールされます。詳細については、『SA ユーザーガイド: プロビジョニング』を参照してください。
- SAサーバーエージェントのバイナリをサーバーにコピーし、手動でインストールします。詳細については、『SAユーザーガイド: Server Automation』を参照してください。

エージェントの登録では、SAは各サーバーに一意のID (マシンID (MID)) を割り当て、このIDをモデルリポジトリに保存します。また、サーバーはMACアドレスでも一意に識別できます。MACアドレスは、ネットワークインタフェースカードに割り当てられている一意の16進数であり、ネットワーク上でのデバイスの物理アドレスとして使用されます。

コアコンポーネント

コアコンポーネントはSAコアの中核であり、サーバーの監視と管理を可能にします。ネットワークサーバーに関する重要な情報の取得、サーバーのプロビジョニング、パッチの適用、サーバーのオンラインまたはオフライン切り替え、サーバーの構成と監査などの操作をユーザーが行う場合、この操作はコアコンポーネントによって制御されます。

次の項では、SAコアコンポーネントとインタフェースについて詳しく説明します。SAコンポーネントが相互に連携してサーバーを管理するしくみについては、
『SA 管理ガイド』を参照してください。

SAコアコンポーネントのバンドル

一部のSAコアコンポーネントはまとめてバンドル化し、標準インストールで1つの単位としてインストールする必要があります。また、バンドルに含まれる一部のコンポーネント (特に、リポジトリストア、OSプロビジョニングメディアサーバー、OSプロビジョニングブートサーバー) は、カスタムインストールを実行して個別に別のホストにインストールすることが可能です。ただし、分散コアコンポーネントなど複雑なインストールにはHPプロフェッショナルサービスやHP認定コンサルタントのサポートが必要になるので、カスタマーインストールではサポートされません。

表 1 は、SAコンポーネントバンドルと構成コンポーネントの例を示します。スライスコンポーネントバンドルには、インスタンスを複数インストールし、負荷分散を実行できます。

SAコアコンポーネントのバンドルには、次のような利点があります。

- 複数サーバーのデプロイメントがシンプルになり、堅牢性も向上します。
- スライスコンポーネントバンドルを追加インストールすることで、水平方向の拡張が可能になります。
- 可用性が向上します。
- 複数のインスタンスをインストールすることで、スライス間で負荷を分散できます。

SAコアコンポーネントのアーキテクチャーとインタラクションの詳細については、SAドキュメントセットに含まれるSA アーキテクチャー図を参照してください (HPセルフソルブからのダウンロードも可能です)。

表1では、SAコアコンポーネントのバンドルをまとめます。

表1　　コンポーネントの区分

モデル リポジトリ	インフラ ストラクチャー コンポーネント	OSプロビジョ ニング コンポーネント	スライス コンポーネント#1	スライス コンポーネント#x
コア あたり1つ	コアあたり1つ	通常はコア あたり1つ	コアあたり1つ	コアあたり複数
モデル リポジトリ	管理ゲートウェイ プライマリデータ アクセスエンジン モデルリポジトリ マルチマスターコ ンポーネント ソフトウェアリポ ジトリストア(別ホ ストに配置可能)	メディアサー バー ブートサーバー	コアゲートウェイ/ エージェントゲート ウェイ コマンドセンター Global File System Webサービスデータア クセスエンジン セカンダリデータア クセスエンジン Build Manager コマンドエンジン ソフトウェア リポジトリ HP Live Network (HPLN) DCML Exchange Tool (DET) ソフトウェアリポジ トリアクセレーター (tsunami) Memcache	コアゲートウェイ/ エージェントゲート ウェイ コマンドセンター Global File System Webサービスデータ アクセスエンジン セカンダリデータア クセスエンジン Build Manager コマンドエンジン ソフトウェア リポジトリ HP Live Network (HPLN) DCML Exchange Tool (DET) ソフトウェアリポジト リアクセレーター (tsunami) Memcache

ブートエージェントは、サーバーエージェントではなく、OSプロビジョニングの一部として機能します。

モデルリポジトリ

モデルリポジトリには、SAが提供するOracleデータベース、またはSAデータベースの要件を満たす既存のOracleインストールが必要です。詳しい要件については、『SA Installation Guide』または『Oracle Setup for the Model Repository』を参照してください。

モデルリポジトリはスタンドアロンのコンポーネントであり、他のコアコンポーネントとはバンドルされません。すべてのSAコンポーネントは、すべてのSA管理対象サーバーについて保持されているデータモデルを使用し、更新します。モデルリポジトリには、次の情報が保存されています。

- SAで管理するすべてのサーバーのインベントリ。
- サーバーに関連付けられているハードウェアのインベントリ(メモリ、CPU、ストレージ容量など)。
- 管理対象サーバーの構成情報。
- 管理対象サーバーにインストールされているオペレーティングシステム、システムソフトウェア、アプリケーションのインベントリ。

- OSプロビジョニングで使用するオペレーティングシステムインストールメディアのインベントリ(メディア本体はOSプロビジョニングメディアサーバーに保存されます)。
- インストール可能なソフトウェアと、ソフトウェアの構成およびインストール方法を制御するソフトウェアポリシーのインベントリ。ソフトウェアインストールメディア本体は、ソフトウェアリポジトリに保存されます。
- 認証とセキュリティの情報。

コアコンポーネントのバンドル

インフラストラクチャーコンポーネントバンドル

- プライマリデータアクセスエンジン

  データアクセスエンジンは、モデルリポジトリに対するXML-RPCインタフェースを提供します。このインタフェースを使用することにより、SA Webクライアント、システムデータの収集、サーバー上の監視エージェントなど、クライアントとのインタラクションを簡単に実行できます。インフラストラクチャーコンポーネントバンドルでインストールされたデータアクセスエンジンは、プライマリデータアクセスエンジンとなります。スライスコンポーネントバンドルでインストールされたデータアクセスエンジンは、セカンダリデータアクセスエンジンとなります。

  モデルリポジトリとのインタラクションはデータアクセスエンジンを経由するので、モデルリポジトリのスキーマに変更を加えてもクライアントへの影響を小さく抑えることができます。また、データアクセスエンジンには、システム全体を変更しなくてもSAに機能を追加できるという利点もあります。

- 管理ゲートウェイ

  他のSAコアやサテライトとの通信を管理します。

- モデルリポジトリ マルチマスターコンポーネント

  モデルリポジトリのマルチマスターコンポーネントは、インフラストラクチャーコンポーネントバンドルと一緒にインストールされます。マルチマスターメッシュにはコアインストールが複数含まれます。したがって、モデルリポジトリのマルチマスターコンポーネントは、モデルリポジトリ内のデータをメッシュ内のすべてのコアで同期し、1つのリポジトリで行った変更内容を他のリポジトリに反映します。

  モデルリポジトリのマルチマスターコンポーネントには、それぞれ送信コンポーネントと受信コンポーネントが存在します。送信コンポーネント(送信モデルリポジトリマルチマスターコンポーネント)は、モデルリポジトリをポーリングし、未発行のトランザクションがあると他のモデルリポジトリに送信します。受信コンポーネント(受信モデルリポジトリマルチマスターコンポーネント)は、他のモデルリポジトリから送信されたトランザクションを受信します。

SA 7.80から、TIBCO Rendezvousに代わってSA Busが提供されています。SA Busは、認定メッセージングサービスを提供するライブラリセットです。

- ソフトウェアリポジトリストア

  ソフトウェアリポジトリストアコンポーネントは、インフラストラクチャーコンポーネントバンドルをホストする任意のサーバーにインストールできます。SA 9.0で、ソフトウェアリポジトリはスライスコンポーネントバンドルの一部となり、スライスコンポーネントバンドルのホストに対するNFSエクスポートを処理するコンポーネントとして、ソフトウェアリポジトリストアが追加されています。

  ソフトウェアリポジトリストアをインストールしない場合、スライスコンポーネントバンドルサーバーがファイルシステムにアクセスするには、NAS(ファイラー)の構成を手動で行う必要があります。

スライスコンポーネントバンドル

- **コマンドエンジン**

  スライスコンポーネントバンドルの一部です。コマンドエンジンは、複数のサーバーに分散したプログラムを実行するシステムです (一般的に、SAサーバーエージェントが使用されます)。コマンドエンジンスクリプトはPythonで記述され、コマンドエンジンサーバーで実行されます。コマンドエンジンスクリプトでは、サーバーエージェントにコマンドを発行することができます。これらの要求は安全に配信され、モデルリポジトリに保存されているデータを使用して監査できます。

  スライスコンポーネントバンドルを複数インストールすると、コマンドエンジンも複数使用できるので、水平方向の拡張性が大幅に向上します。コマンドエンジンインスタンスが複数ある場合、スライスコンポーネントバンドルが備えるロードバランシング機能を使ってコマンド送信とスクリプト実行に伴う負荷を分散できます。また、フェイルオーバーと高可用性の機能も向上します。たとえば、コマンドエンジンインスタンスがクラスター内の別ノードにコマンド処理を切り替えようとしたとき、そのノードがダウン状態の場合には次のノードにフェイルオーバーできます。

  SAでは、コマンドエンジンのスクリプトを使用して機能を実装します。

- **ソフトウェアリポジトリ**

  スライスコンポーネントバンドルの一部です。このリポジトリには、ソフトウェア/アプリケーションのプロビジョニングと修復を行うバイナリ/パッケージ/ソースをアップロードして保存しておきます。関連コンポーネントの1つにソフトウェアリポジトリストアがあります。このストアはインフラストラクチャーコンポーネントバンドルと一緒にインストールされ、スライスコンポーネントバンドルのホストに対するNFSエクスポートを処理します。

  SAは、ソフトウェアリポジトリのミラーリングをサポートします。メッシュ内でミラーとして使用するソフトウェアリポジトリと、ジョブをミラーリングする頻度は、SA Web クライアントの構成パラメーターで制御できます。また、ミラーリングによって、サテライトのソフトウェアリポジトリキャッシュが影響を受けることはありません。

  ソフトウェアリポジトリミラーリングには、大量のディスク容量が必要になります。ミラーリングは、標準インストール時と高度なインストール時に無効にすることができます (デフォルトでは有効)。

  ソフトウェアリポジトリミラーリングの構成については、『SA 管理ガイド』を参照してください。

  ソフトウェアパッケージをSAライブラリにアップロードする方法については、『SAユーザーガイド: ソフトウェア管理』を参照してください。

- **コアゲートウェイ/エージェントゲートウェイ**

  コアゲートウェイは、エージェントゲートウェイと直接通信することにより、コアコンポーネントとの間で要求の送信と応答を行います。

- **コマンドセンター**

  コマンドセンター (OCC) は、SA Webクライアントの基盤となるコアコンポーネントです。OCCには、HTTPSプロキシサーバーとアプリケーションサーバーが含まれます。OCC には、SA Web クライアントを経由しないとアクセスできません。

- **DCML Exchange Tool**

  DCML Exchange Toolはスライスコンポーネントバンドルと一緒にインストールされるツールであり、SAコンテンツのインポートとエクスポートを実行します。詳細については、『SA コンテンツユーティリティガイド』を参照してください。

- **Global File System**

  Global File System (OGFS) は、スライスコンポーネントバンドルと一緒にインストールされ、一元的な実行環境をSAに提供します。

  OGFS は、1つまたは複数の物理サーバーで実行できます。したがって、スライスコンポーネントバンドルをコアに追加していくだけで、SAの実行容量を拡張することが可能になります。

OGFSは、SAビルトインコンポーネントとユーザーが記述したプログラムの両方を仮想ファイルシステム内で実行します。仮想システムは、SAデータモデル、SAアクション、管理対象サーバーを仮想のファイルとディレクトリとして提示します。

これはSA固有の機能であり、Global Shellと自動化プラットフォーム拡張(APX)のユーザーは、任意のスクリプト言語やプログラミング言語を使用してSAデータのクエリ実行やサーバー管理を実行できます。OGFSはすべてのデータ、アクション、管理対象サーバーのアクセスをSAセキュリティモデルを使ってフィルター処理するので、OGFSで実行するプログラムのセキュリティはデフォルトで確保されます。

- **Webサービスデータアクセスエンジン**

  Webサービスデータアクセスエンジンは、モデルリポジトリに対するパブリックオブジェクトの抽象化レイヤーを提供し、これによって他のSAコアコンポーネントのパフォーマンスを向上します。このオブジェクト抽象化には、Simple Object Access Protocol (SOAP) API、サードパーティの統合コンポーネント、SAコンポーネント(SA Webクライアントなど)のバイナリプロトコルでアクセスできます。

- **セカンダリデータアクセスエンジン**

  データアクセスエンジンは、モデルリポジトリに対するXML-RPCインタフェースを提供します。このインタフェースを使用することにより、SA Webクライアント、システムデータの収集、サーバー上の監視エージェントなど、クライアントとのインタラクションを簡単に実行できます。インフラストラクチャーコンポーネントバンドルでインストールされたデータアクセスエンジンは、プライマリデータアクセスエンジンとなります。スライスコンポーネントバンドルでインストールされたデータアクセスエンジンは、セカンダリデータアクセスエンジンとなります。

  モデルリポジトリとのインタラクションはデータアクセスエンジンを経由するので、モデルリポジトリのスキーマに変更を加えてもクライアントへの影響を小さく抑えることができます。また、データアクセスエンジンには、システム全体を変更しなくてもSAに機能を追加できるという利点もあります。

- **Build Manager**

  Build ManagerはSA OSプロビジョニングの一部ですが、スライスコンポーネントバンドルと一緒にインストールされます。Build ManagerはOSビルドエージェントとコマンドエンジンの間の通信をサポートする機能を持ち、コマンドエンジンが送信したOSプロビジョニングコマンドを受信します。また、OSプロビジョニング手順を実行できるように、プラットフォーム固有のビルドスクリプトの実行時環境を提供します。

- **HP Live Network (HPLN)**

  HP Live Networkは、Server Automation (SA)、Network Automation (NA)、Client Automation (CA)、Operations Orchestration (OO)、Service Automation Reporter (SAR)で提供されたコンテンツ更新を配信します。また、セキュリティポリシーとコンプライアンスポリシーを提供することを通じて、SA、NA、CAへの投資効果を最大限に引き出し、拡張可能な自動化プラットフォームで新しい自動化機能を継続的に提供します。

  HPLNは、SAコアのインストール時にスライスコンポーネントバンドルと一緒にインストールされます。

- **ソフトウェアリポジトリアクセレーター(tsunami)**

  オブジェクトストアのダウンロードアクセラレーターであり、LinuxベースのSAコアと直接通信するエージェントの修復パフォーマンスと拡張性を向上します。

  パフォーマンスと拡張性は、主に次の2つの部分で向上します。

  — RPM修復分析: RPM依存関係の分析/プレビューでパッケージヘッダーを取得します。SAの旧リリースよりプレビューが格段に高速になっています。

  — 修復パッケージのステージング: ソフトウェアリポジトリから管理対象ホストをダウンロードする処理が、SAの旧リリースより格段に高速になり、10GbEネットワーキングにも対応しています。

- **memcache**

  メモリ内のキャッシュレイヤーであり、ソフトウェアリポジトリアクセレーター(`tsunami`)コンポーネントと連携して、LinuxベースのSAコアと直接通信するエージェントでの修復と拡張性を向上します。

OSプロビジョニングコンポーネントバンドル

- **ブートサーバー**

  ブートサーバーは、SA OSプロビジョニングの一部です。inetbootよりSunシステムの、PXEよりx86システムのネットワークブートをサポートします。このサポートを提供するプロセスには、Internet Software ConsortiumのDHCPサーバーが使われています。

- **メディアサーバー**

  メディアサーバーは、SA OSプロビジョニングの一部です。OSプロビジョニング時に、ベンダーが提供するメディアへのネットワークアクセスをサポートします。このサポートを提供するプロセスには、Samba SMBサーバーとLinux NFSが含まれます。有効なオペレーティングシステムインストールメディアをメディアサーバーにコピーおよびアップロードします。

OSビルドエージェント: OSビルドエージェントは、OSプロビジョニングの一部です。プレプロビジョニング(ネットワークブート)プロセスで実行され、Build Managerを使用してサーバーをSAコアに登録し、OSインストールプロセスを実行します。

サテライトインストール

- **ソフトウェアリポジトリキャッシュ**

  ソフトウェアリポジトリキャッシュには、コアのソフトウェアリポジトリ(または別のサテライト)のコンテンツのローカルコピーが保存されています。ソフトウェアリポジトリのローカルコピーを保存しておくことによって、サテライトの管理対象サーバーにソフトウェアをインストールまたは更新する際、パフォーマンス向上やネットワークトラフィック低減などの効果を期待できます。

- **サテライトエージェントゲートウェイ**

  サテライトエージェントゲートウェイは、サテライトとコア間の通信を、コアの管理ゲートウェイ経由で処理します。

SAゲートウェイ

SAゲートウェイは、管理対象サーバーとSAコアの間の通信、複数コア(マルチマスターメッシュ)間の通信、サテライトインストールとSAコア間の通信を管理します。マルチマスターインストールについてはマルチマスターメッシュ (複数コア) (35ページ)、サテライトインストールについてはSA サテライト (38ページ)を参照してください。

ゲートウェイには、次のタイプがあります。

- **管理ゲートウェイ**

  このゲートウェイは、SAコア間の通信と、SAコアとサテライト間の通信を管理します。

- **コアゲートウェイ/エージェントゲートウェイ**

  このゲートウェイは相互に連携して、SAコアと管理対象サーバー上のSAエージェント間の通信を管理します。

- **サテライトゲートウェイ**

  このゲートウェイは、ユーザー構成に応じて、管理ゲートウェイまたはコアゲートウェイを経由してSAコアと通信します。

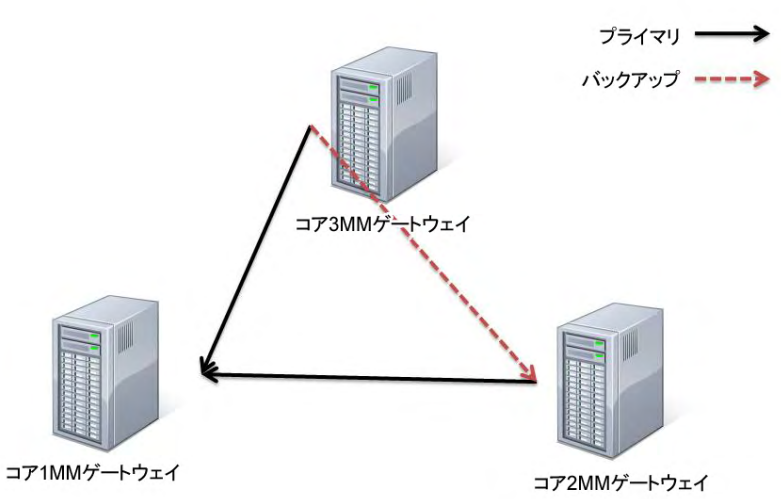
マルチマスターのマスターゲートウェイバックアップルート

マルチマスターメッシュでコアを3つ以上インストールすると、第2コアへのバックアップルートが自動作成されます (デフォルト)。これにより、第1コアにはプライマリルート、第2コアにはバックアップルートが確保されます。ゲートウェイバックアップルートは、SAによってインストール時に自動作成されるので、構成情報の指定は必要ありません。ただし、SA がバップアップルートを作成できない場合は、HP テクニカルサポートへの問い合わせを指示するメッセージが表示され、ゲートウェイバックアップルートの手動作成が必要になることがあります。

ゲートウェイバックアップルートが作成されるのは、SA 9.0 の新規インストール時のみで、アップグレードでは作成されません。旧バージョンから SA 9.0 へのアップグレードでは、ゲートウェイバックアップルートは作成されません。したがって、手動での作成が必要になります。詳細については、HPテクニカルサポートに連絡してください。

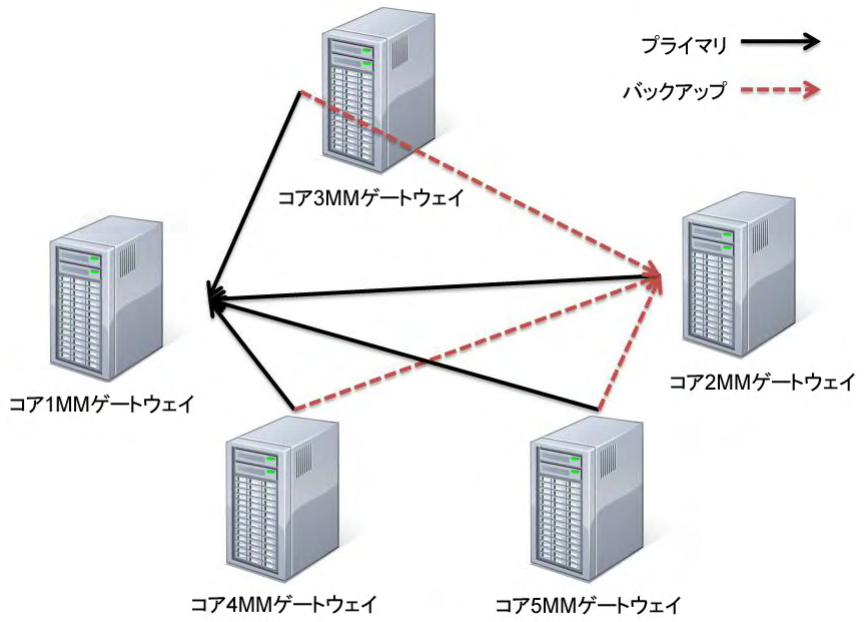
たとえば、メッシュにコアが3つ以上ある場合、すべてのマルチマスタートラフィックは第1コアのマスターゲートウェイを経由します (デフォルト)。ただし、第1コアのマスターゲートウェイに障害が発生した場合、第 2 コアのマスターゲートウェイがバックアップのマスターゲートウェイとしてデフォルトで指定されています。これ以降メッシュに追加したコアのマスターゲートウェイは、インストールした順序でバックアップとして指定されます。インストールでは、3 番目以降のコアにデフォルトで 2 つのトンネルが設定されます。最初のトンネルは第1コアのマスターゲートウェイ、2番目のトンネルはメッシュ内の第2コアと通信します。図5を参照してください。

図5　　コアが3つ、バックアップルートが1つの場合



メッシュにマスターゲートウェイが複数あると、バックアップルートも冗長化されます。図6を参照してください。

図6　　コアが5つ、バックアップルートが複数ある場合



マスターゲートウェイに障害が発生すると、デフォルトで、バックアップルートが自動的にマルチマスターメッシュのトラフィックを処理します。故障したマスターゲートウェイがオンラインに復帰すると、メッシュトラフィックが再びこのゲートウェイを通過するように自動的にルートが戻ります。

SAのトポロジ

SAトポロジは、ファシリティのニーズに最適なものを選ぶ必要があります。ここでは、SAトポロジを選択する際に必要になる内容について説明します。

単一ホストコア

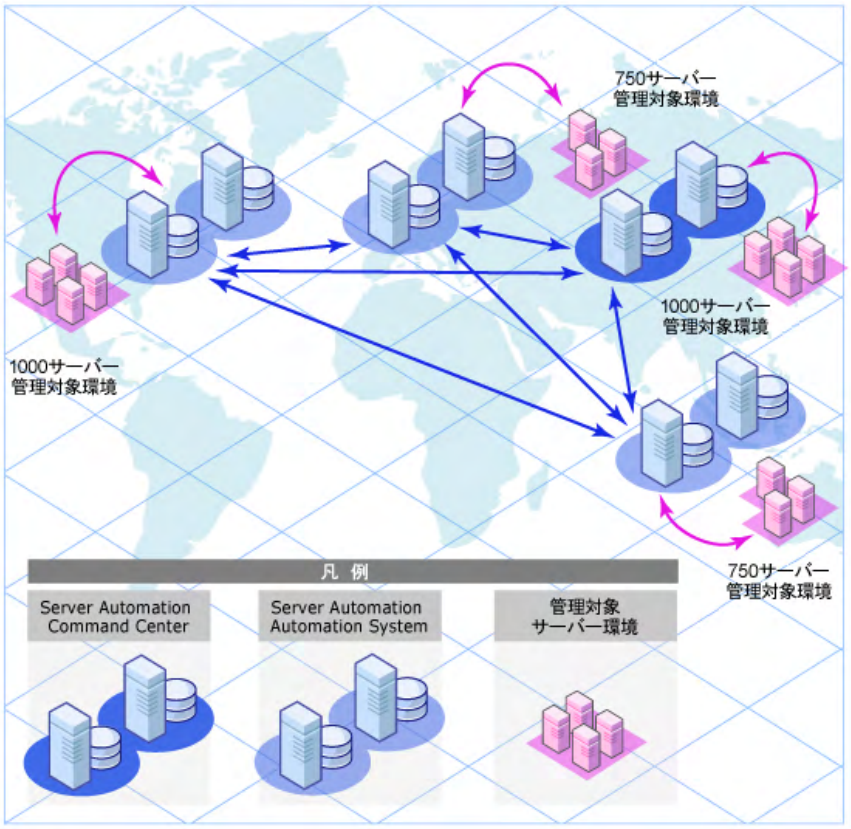
単一ホストコア(以前はスタンドアロンコアと呼ばれていました)は最もシンプルなトポロジであり、1つのファシリティでサーバーを管理します。

単一ホストコアは、小規模なサーバーネットワークを1つのファシリティで管理する場合に最適です。単一ホストコアは他のSAコアと通信することはありませんが、必要に応じて、マルチマスターメッシュの一部として構成を変換できます。

マルチマスターメッシュ(複数コア)

複数のファシリティでサーバーを管理するには、SAコアのマルチマスターメッシュをインストールします。これは、複数のSAコアとサテライトを組み合わせたものです。

図7　　マルチマストートポロジ



マルチマスターメッシュとは、管理ゲートウェイを介して相互通信する複数のSAコアで構成され、モデルリポジトリに保存されている管理対象サーバー関連データを同期することができます。マルチマスターメッシュ内にあるモデルリポジトリのデータが変更されると、変更内容がメッシュ内にある他のモデルリポジトリにブロードキャストされ、同期されます。

各モデルリポジトリの変更内容を他のすべてのモデルリポジトリに反映して同期するSAコアコンポーネントは、モデルリポジトリマルチマスターコンポーネントと呼ばれ、インフラストラクチャーコンポーネントバンドルに含まれます。このレプリケーション機能を使用することによって、ソフトウェアと環境の属性を含む「ブループリント」を各ファシリティに保存および保持できるので、インフラストラクチャーの再構築も簡単に行うことができます。また、追加容量のプロビジョニングや更新の配信に加え、ソフトウェアビルド、テンプレート、依存関係を複数のファシリティで共有する操作も簡単に実行できます。

マルチマスターメッシュには、サテライトインストールも含まれます。

サーバーは、SAコアをインストールした任意のファシリティから、SA Webクライアントまたは SAクライアントを使用して管理できます。

マルチマスターメッシュの利点

マルチマスターメッシュには、特に次のような利点があります。

- 一元管理: マルチマスターメッシュ内の管理対象サーバーは、メッシュ内にあるSAコアで管理する任意のファシリティから一元管理できます。管理できる範囲は1箇所に限定されることはなく、地理的な制約もありません。
- 冗長化: データ管理をファシリティ間で同期(レプリケーション)することで、冗長化を図ることができます。たとえば、メッシュ内のあるファシリティに含まれるSAコアに障害が発生した場合、マルチマスターメッシュ内の他のコアに管理対象サーバーのコピーデータが保存されているので、これを元に、破損したコアのモデルリポジトリを前回の正常稼働状態に復元することができます。さらに、破損したコアが使用できなくなる間、メッシュ内の他のコアは中断することなく稼働を継続できます。

  また、レプリケーションによって、メッシュ内にあるファシリティの稼働を中断することなく、ファシリティの停止や追加を行うことができます。
- パフォーマンスの拡張: マルチマスターメッシュでは、マルチマスターデータベースの同期データのみがネットワーク経由で転送されるので、ネットワーク帯域幅にかかる負荷を軽減できます。
- 地理的な条件に依存しない: ネットワークが中断しても、場所に関係なくコアはサーバー管理を継続できます。

ファシリティとレルム

SAゲートウェイは、ネットワークトラフィックのルーティングを行うコンストラクトと、IPアドレスの競合を回避するコンストラクトを使用します。

ファシリティ

ファシリティとは一般的に、モデルリポジトリに保存されている管理対象環境のデータに基づいて、1つのSAコアが管理するサーバーの集まりを表すコンストラクトです。一般的にファシリティは、地理的な場所(たとえば、サニーベール、サンフランシスコ、ニューヨーク、さらには特定のデータセンターなど)を表します。

ファシリティはSA内でのアクセス権の境界であり、ユーザーは1つのファシリティ内でのアクセス権を別のファシリティで適用することはできません。管理対象サーバーはそれぞれが1つのファシリティに割り当てられます。デバイスは、最初にSAコアに登録する際、登録で使用するゲートウェイに関連付けられているファシリティに割り当てられます。

たとえば、Admin Aというユーザーがサニーベールでサーバーパッチの管理を担当しているとします。ファシリティという枠組みの中では、Admin Aはサニーベールというファシリティにユーザーとして割り当てられます。Admin Aがサーバーを表示すると、サニーベールに割り当てられているサーバーのみが表示され、他のファシリティのサーバーは表示されません。

ファシリティには、次の2つのタイプがあります。

- **コアファシリティ**

  各SAコアには、コアファシリティが1つ存在します。
- **サテライトファシリティ**

  サテライトをインストールするときに作成されるデフォルトのファシリティです。

レルム

レルムとはSAコンストラクトの1つであり、これによってSAは、1つのファシリティ内にある異なるネットワーク上のサーバーを、IPアドレスが競合している場合でも管理できます。レルムとは、ファシリティのネットワーク内にあるデバイスのIPアドレスに付加される一意のIDです。これに基づいて、SAゲートウェイはマルチマスターメッシュ内の各ネットワーク上にあるデバイスを一意に識別するので、IPアドレスが競合している場合にも対応できます。

レルムはIP名前空間を定義する論理エンティティであり、この名前空間内では管理対象サーバーのIPアドレスはすべて一意である必要があります。ただし、サーバーのレルムが異なるとIPアドレスが重複する可能性がありますが、レルムのメンバーシップによってSA内では一意に識別されます。

レルムは、ゲートウェイによって相互接続されてゲートウェイメッシュを構成し、これは相互接続された単一のSAゲートウェイネットワークとして機能します。

インストール時に新しいファシリティを作成して名前を付けると、ファシリティと同じ名前でレルムが作成されます(デフォルト)。たとえば、Datacenterという名前のファシリティを作成すると、Datacenterという名前のレルムも作成されます。このファシリティでさらに続けてレルムを作成すると、Datacenter001、Datacenter002、などの名前が割り当てられます。各レルム内の管理対象サーバーは、レルムの名前とIPアドレスの組み合わせによって一意に識別されます。

マルチマスターメッシュのトポロジの例

図8は、サンフランシスコとロサンゼルスという2つのファシリティにインストールされているコアを含むマルチマスターメッシュを示しています。各ファシリティのコアにはモデルリポジトリが存在し、両方のファシリティ内にある管理対象サーバーに関するデータが保存されています。このデータは、両方のファシリティのモデルリポジトリ間で、定期的に同期(レプリケーション)されます。コアはそれぞれの管理ゲートウェイ経由で通信します。

ロサンゼルスのファシリティ内にある管理対象サーバーから、サンフランシスコのコアへの通信は、ロサンゼルスのエージェントゲートウェイを経由してコアゲートウェイ、さらにロサンゼルスの管理ゲートウェイへと転送されます。さらにこの管理ゲートウェイは、サンフランシスコの管理ゲートウェイとコアゲートウェイを経由して、サンフランシスコのコアと通信します。

図8　　2つのコアを含むマルチマスターメッシュ

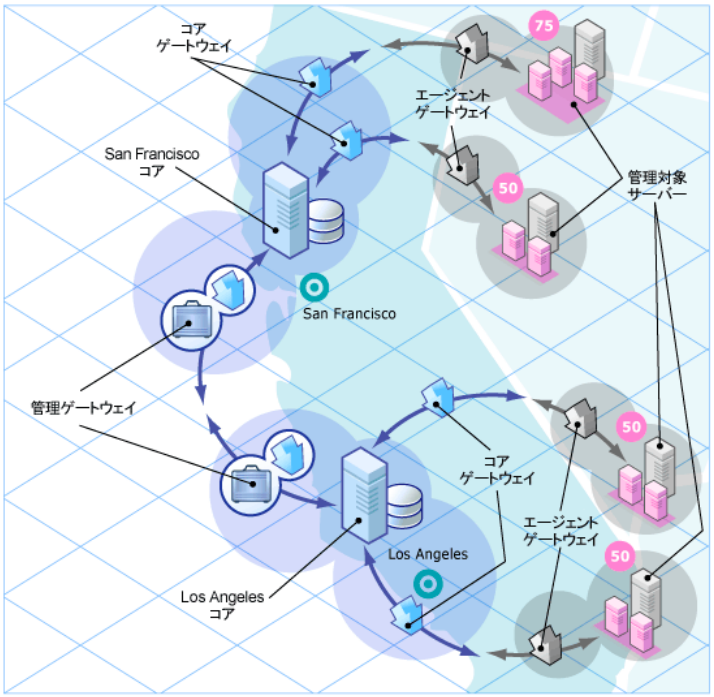


図9は、4つのコアを含むマルチマターメッシュを示します。このメッシュトポロジはスター型と呼ばれるものであり、メッシュの中心にサンフランシスコのコアがあります。SAのインストーラーは、スタートポロジでマルチマスターメッシュを構成するときに、デフォルトでバックアップゲートウェイルートを設定します。

図9　　4つのコアを含むマルチマスターメッシュ

SA サテライト

サテライトは、管理対象サーバーの数が少なく完全なSAコアインストールを必要としないリモートサイト向けのソリューションです。サテライトでは、ホストに最小限必要なコアコンポーネントのみをインストールでき、ホストからプライマリコアのデータベースとその他サービスにSAゲートウェイ接続経由でアクセスします。

また、限られたネットワーク接続を使ってプライマリファシリティと接続する場合には、帯域幅の問題を軽減することもできます。サテライトで使用するネットワーク帯域幅の上限となるビットレートを指定することができます。これにより、サテライトのネットワークトラフィックによって、同じパイプ上にある他の重要なシステムのネットワーク帯域幅要件が影響を受けることがなくなります。

一般的に、サテライトの最低構成にはサテライトゲートウェイとソフトウェアリポジトリキャッシュが含まれますが、リモートファシリティでサーバー管理機能をフル装備することも可能です。ソフトウェアリポジトリキャッシュには、サテライト内の管理対象サーバーにインストールされているソフトウェアパッケージのローカルコピーが格納され、サテライトゲートウェイは、プライマリコアとの通信を処理します。

オプションで、OSプロビジョニングブートサーバーとメディアサーバーをサテライトホストにインストールし、リモートOSプロビジョニングをサポートすることが可能です。ただしサテライトホストには、これ以外のコンポーネントはインストールできません。サテライトのインストールの詳細については、第9章を参照してください。

サテライトトポロジの例

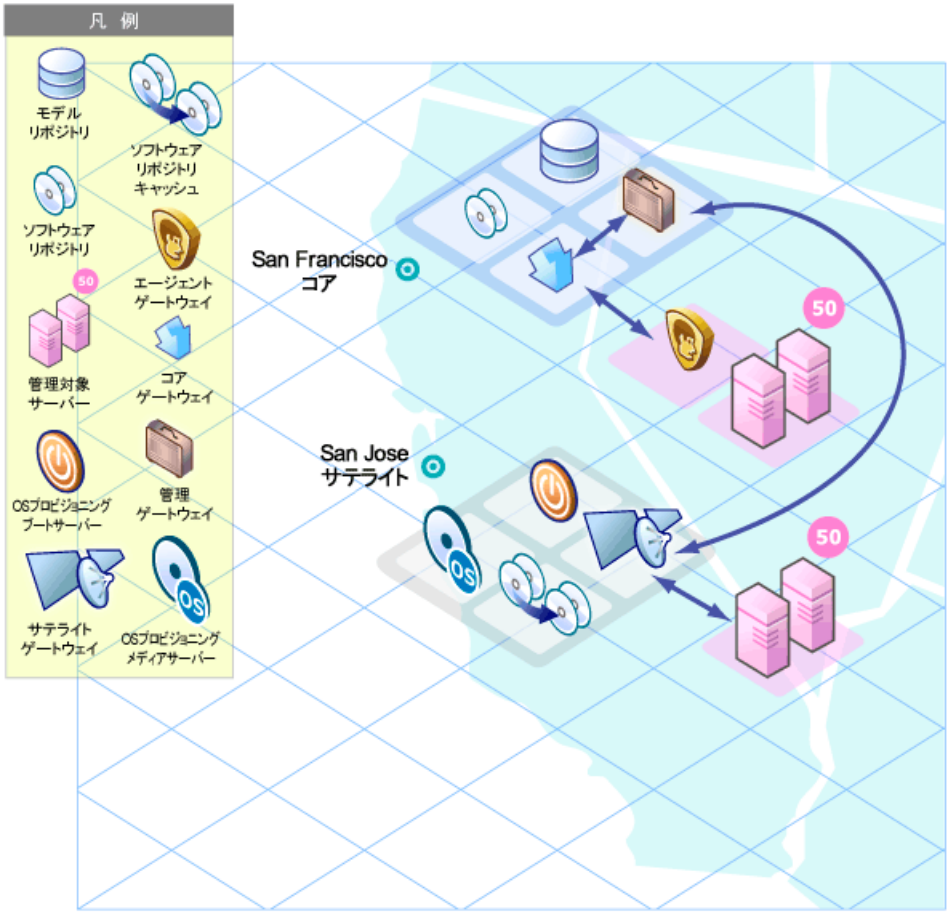
シンプルな単一コアとサテライトのリンク

図10では、単一のサテライトが単一のコアにリンクされています。この例では、サンフランシスコにメインファシリティがあり、これよりも小規模なリモートファシリティがサンノゼにあります。

サンフランシスコの単一コアにはいくつかのコンポーネント (ソフトウェアリポジトリ、モデルリポジトリ、エージェントゲートウェイ、管理ゲートウェイ) が含まれます。この図では、簡略化のために、コマンドエンジンなど一部コアコンポーネントが省略されています。

サンノゼのサテライトには、ソフトウェアリポジトリキャッシュ、サテライトゲートウェイ、オプションのOSプロビジョニングブートサーバーとメディアサーバーが含まれます。

図10　　単一コアのサテライト



サンノゼのサテライトのソフトウェアリポジトリキャッシュには、ファシリティ内の管理対象サーバーにインストールするソフトウェアパッケージのローカルコピーが格納されています。

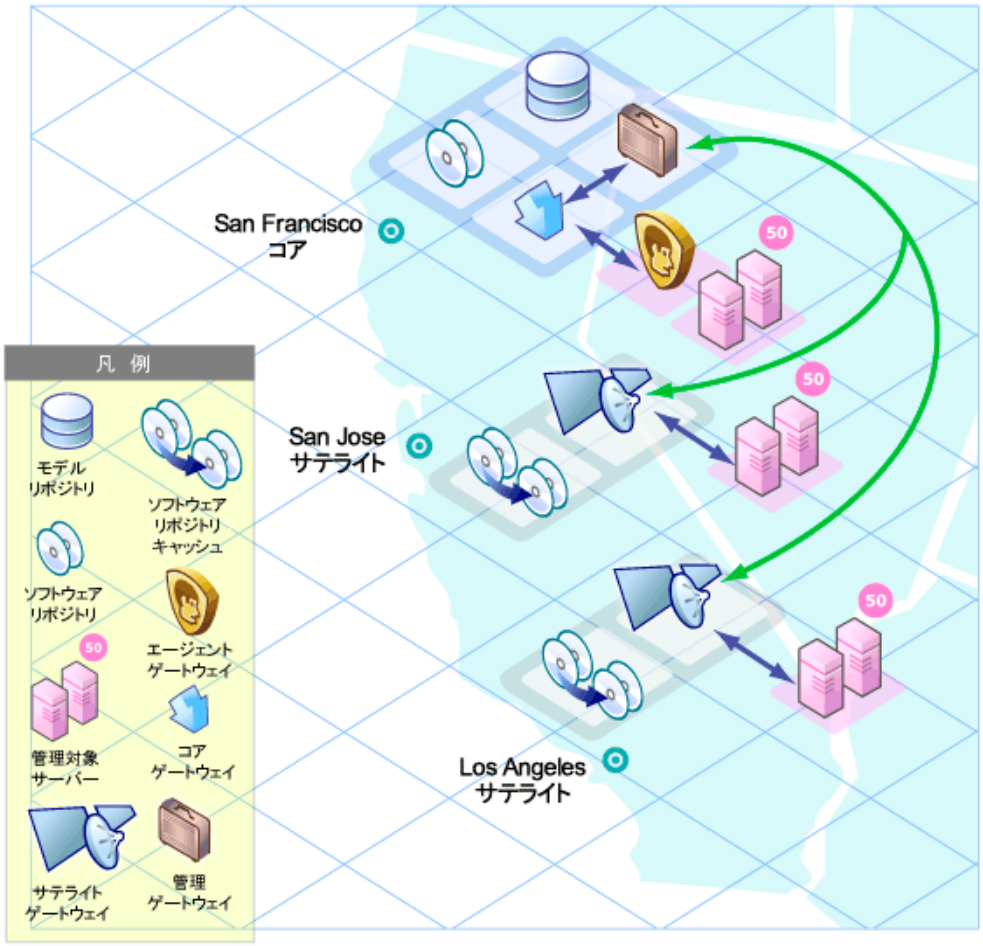
サンノゼのファシリティにある管理対象サーバーにインストールされているサーバーエージェントは、サンフランシスコのコアにサンノゼのサテライトゲートウェイ経由で接続します。このゲートウェイは、サンフランシスコの管理ゲートウェイと通信し、そこからサンフランシスコのコアゲートウェイを経由して、目的のコアコンポーネントへとつながります。

応答の通信では、このパスが逆方向になります。サンフランシスコのファシリティ内にある管理対象サーバーにインストールされているサーバーエージェントは、サンフランシスコのファシリティのエージェントゲートウェイとコアゲートウェイを経由してコアコンポーネントと通信します。

単一コアにリンクする2つのサテライト

図11では、2つのサテライトが単一のコアにリンクしています。この例では、サンフランシスコがメインファシリティであり、サニーベールとサンノゼはサテライトファシリティです。

図11　　単一コアと2つのサテライト

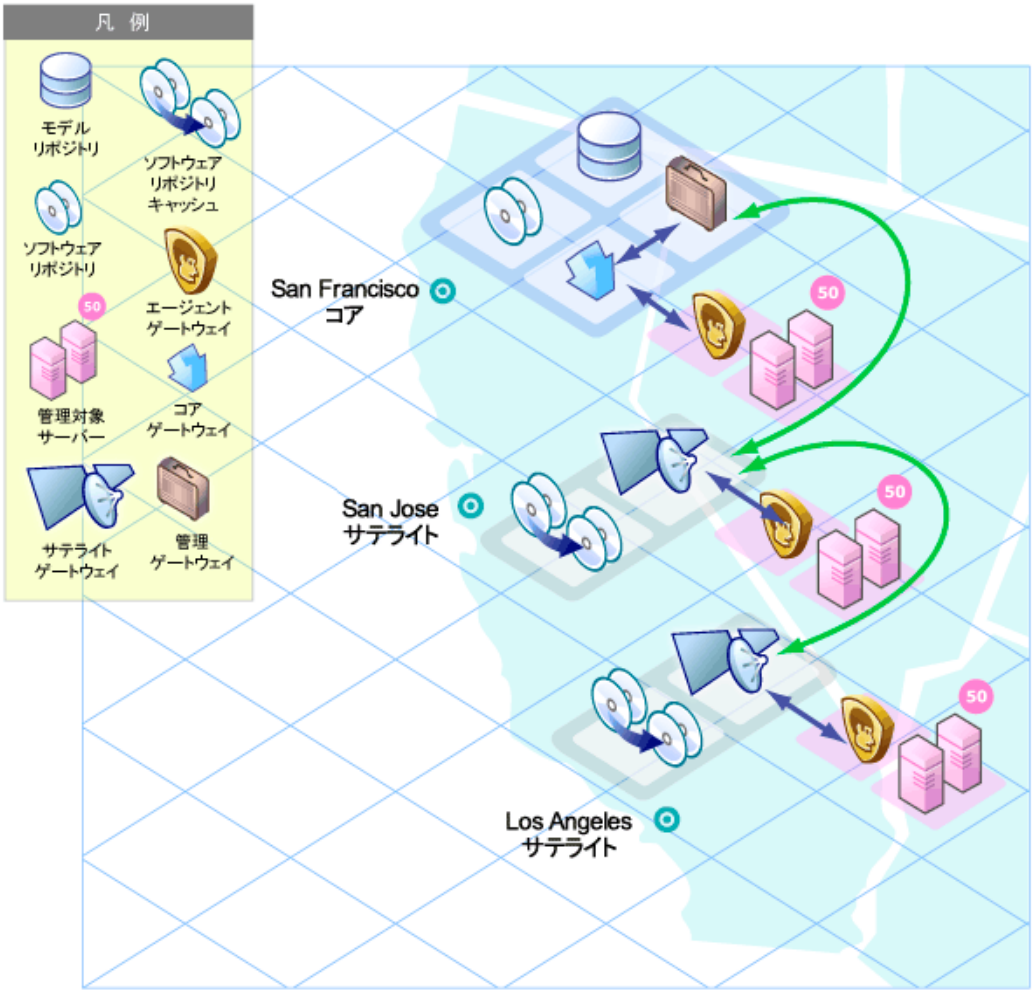


サテライトリンクのカスケーディング

図12は、サテライトのカスケーディングを示しています。このトポロジでは、サテライトゲートウェイがチェーン状に接続されています。このトポロジでは、ソフトウェアリポジトリキャッシュの階層化が可能です。また、このトポロジではサテライトゲートウェイを異なるSAレルムに割り当てる必要がある点に注意してください。

ロサンゼルスのファシリティにある管理対象サーバーにパッケージをインストールする場合、SAはまず、ロサンゼルスのソフトウェアリポジトリキャッシュ内にパッケージが格納されていないかチェックします。パッケージがロサンゼルスにない場合、SAはサンノゼのソフトウェアリポジトリキャッシュをチェックします。サンノゼにもパッケージがない場合、SAはサンフランシスコのコアのソフトウェアリポジトリを確認します。詳細については、『SA 管理ガイド』の「サテライトのソフトウェアリポジトリキャッシュの管理」を参照してください。

図12　　単一コアでのサテライトのカスケーディング



マルチマスターメッシュ内のサテライト

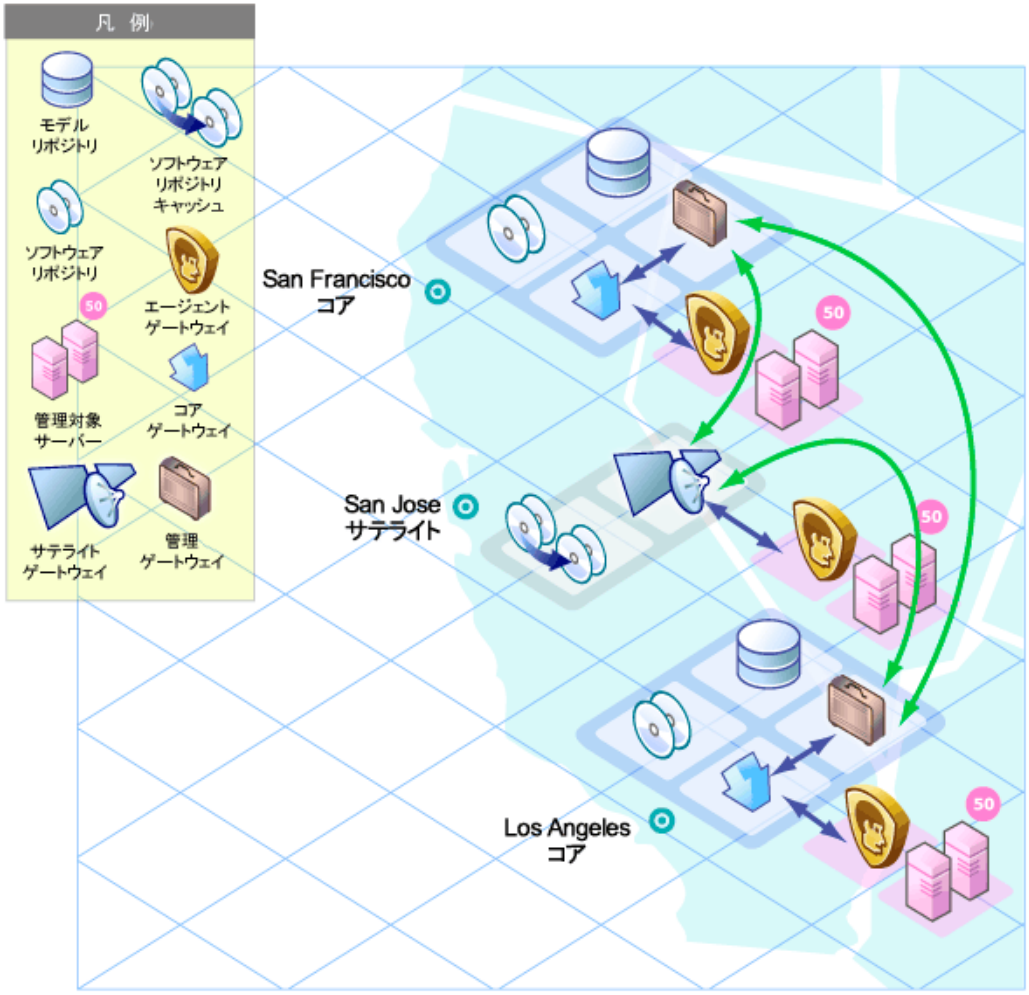
図13では、マルチマスターメッシュ内にある2つのSAコアにサンノゼのサテライトが接続しています。

ロサンゼルスとサンフランシスコの両方に通信可能な場合、管理ゲートウェイはコストが低い方（図13ではサンフランシスコのルート）を選択します。コスト評価は、ゲートウェイのインストールで指定したパラメーターで制御します。システム設計者は、ネットワーク接続コストが最小になるのはどのSAゲートウェイルートなのかを指定するルールを定義できます。

フェイルオーバーシナリオで使用したサンプル環境を使用する場合、正常稼働時には、サンノゼのサテライトにあるサーバーはサンフランシスコのコアによって管理されます。ただし、サンフランシスコとロサンゼルスのコアは、それぞれの管理ゲートウェイを経由して直接接続しています。

サンノゼのサテライトとサンフランシスコのコア間の接続が切断されると、サンノゼのサテライトゲートウェイはすぐに、サンフランシスコからロサンゼルスのコアへと通信を移動します。これにより、コアはサンノゼのサーバー管理を継続できます。サンフランシスコのコアのモデルリポジトリのデータは、通常のSAオペレーションでロサンゼルスのモデルリポジトリに複製されるので、ロサンゼルスのコアにはサンノゼサイトの最新情報が格納されます。

図13　　マルチマスターメッシュ内のサテライト



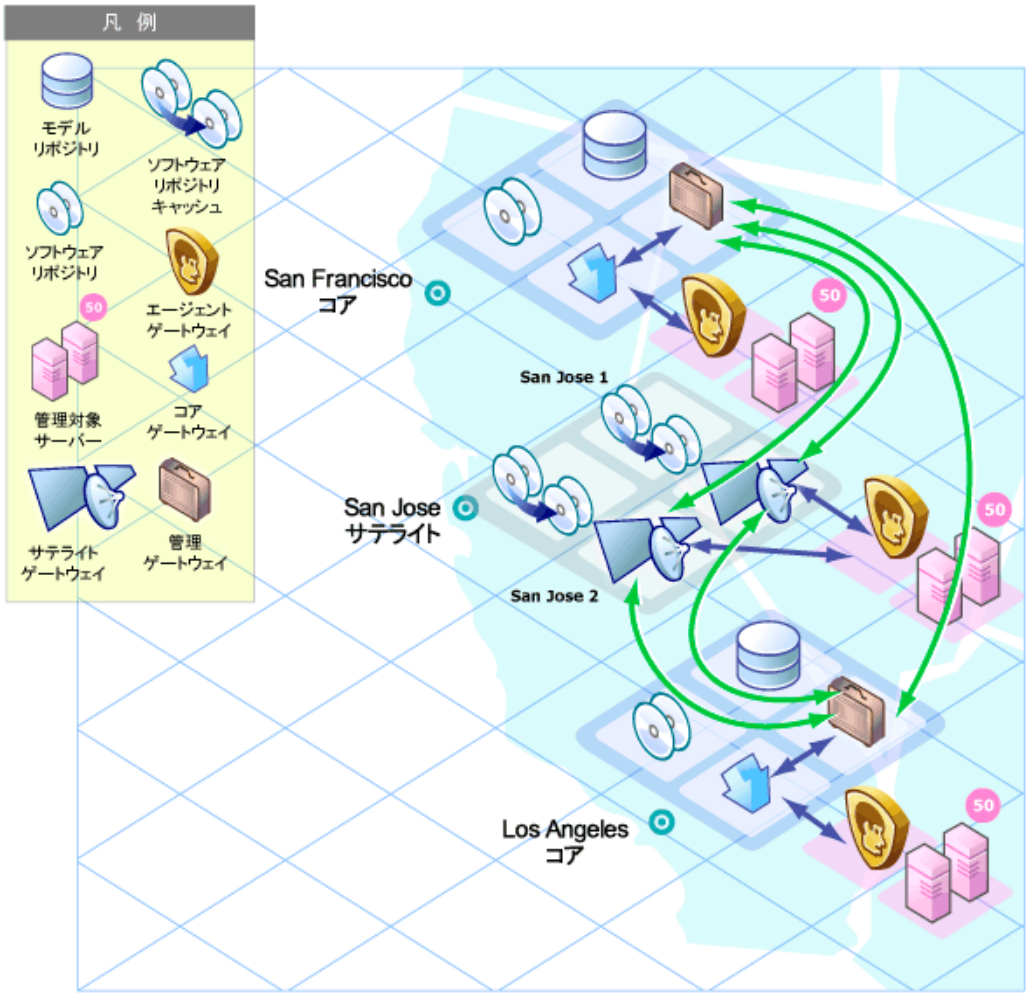
マルチマスターメッシュで複数のゲートウェイを持つサテライト

図14は、2方向でフェイルオーバーを実行できるトポロジの例です。まず、サンノゼのサテライト1と2には、サンフランシスコとロサンゼルス両方の管理ゲートウェイにつながるゲートウェイ接続があります。ロサンゼルスのコアが利用不可になった場合、サンフランシスコのコアがサンノゼのサテライトにあるサーバーを管理します。

次に、サンノゼのファシリティ内にある管理対象サーバーにインストールされているエージェントは、サテライトの両方のエージェントゲートウェイをポイントしています。SAエージェントは、利用不可なエージェントゲートウェイに対して自動的に負荷分散するので、サンフランシスコまたはロサンゼルスのコアと直接通信できます。

いずれかのゲートウェイが利用不可になった場合、利用不可なゲートウェイをプライマリゲートウェイとするエージェントは、セカンダリゲートウェイへと自動的にフェイルオーバーします。通常のエージェントとコア間の通信では、SAエージェントはサテライトに新しく追加(または削除)されたゲートウェイを検出します。

図14　　マルチマスターメッシュで複数のゲートウェイを持つサテライト



SAの製品オプション

SAでは、さまざまなITプロセスを自動化するオプションが提供されています。

- Server Automation Visualizer (SAV)
- Storage Visibility and Automation
- レポート

Server Automation Visualizer (SAV)

Server Automation Visualizer (SAV) は、IT環境内に分散したビジネスアプリケーションについて、オペレーションアーキテクチャーと動作に関する情報提供と管理を効率的に行います。分散ビジネスアプリケーションは、多くのサーバーで実行されるサービス、ネットワーク、ストレージデバイスを含む複雑な構成なので、相互の関連性、パフォーマンス低下の原因、トラブルシューティングと問題解決の方法、環境の変更がもたらす結果を把握することはますます難しくなっています。

SAVでは、このような情報を物理的な側面と論理的な側面からグラフィック表示します。

Storage Visibility and Automation

Storage Visibility and Automation は、ストレージサプライチェーン全体の表示と管理をエンドツーエンドに実行することによってストレージ管理を行います。Storage Visibility and Automation は、アプリケーションストレージ、依存関係と可視化、ストレージの監査、ストレージの容量と利用率のトレンド分析、スクリプト作成と自動化などのコスト削減ツールを提供することによって、サーバー管理者が日々行う作業をサポートします。詳細については、『Storage Visibility and Automationユーザーガイド』を参照してください。

レポート

SA のレポートでは、環境内の管理対象サーバー、ネットワークデバイス、ソフトウェア、パッチ、カスタマー、ファシリティ、オペレーティングシステム、コンプライアンスポリシー、ユーザーとセキュリティに関する包括的な情報がリアルタイムで提供されます。レポートはグラフと表の形式で提示され、ポリシーや監査などのレポート内のオブジェクトに対して適切なアクションを実行できるようになっています。また、組織で使用しやすいファイル形式 (`.html`と`.xls`) でローカルファイルシステムにエクスポートもできます。

SAユーティリティ

SAでは、データセンターで一般的に実行される自動化タスクをサポートするユーティリティが提供されています。

スクリプト実行

SAに付属するスクリプト実行機能では、SAで管理するサーバーファーム全体で、アドホックスクリプトや保存済みスクリプトを共有および実行できます。

手動ではなくSAを使用してスクリプトを実行する方法には、次のような利点があります。

- 多数のUNIXまたはWindowsサーバーでスクリプトを並列実行することにより、時間を節約できるだけでなく、一貫性を維持できます。
- 役割ベースのアクセス制御を適用することで、承認した管理者のみに、アクセス権を持つホストでのスクリプト実行を許可します。
- プライベートライブラリとパブリックライブラリにスクリプトを保存し、スクリプトのアクセス制御を行います。
- スクリプト出力の表示とダウンロードを行います。サーバーごとのレポート、またはすべてのサーバーの出力を1箇所に集約したレポートを作成します。

- スクリプトの一括カスタマイズが可能です。管理者は、SAに保存されているサーバーの環境と状態に関する情報にアクセスできます。これは、適切なサーバーで適切なスクリプトを実行する上で非常に重要な機能です。
- 包括的な監査証跡を作成し、各スクリプトの実行者と実行日時を記録します。
- システムの状態や構成情報をベースに、スクリプト実行をカスタマイズできます。SAには、サーバーを所有するカスタマーやビジネス、サーバーがステージングサーバーか運用サーバーかの区別、サーバーが設置されているファシリティ、カスタマイズした名前と値のペアなどさまざまな情報が保存されているので、これを参照またはアクセスすることでスクリプトをカスタマイズします。
- セキュリティを損なわない方法でスクリプトを共有できます。SAでは、スクリプト実行を許可するユーザーと対象サーバーのアクセス制御が厳格に実施され、スクリプト実行の監査証跡が作成されるので、セキュリティを損なわずにスクリプトを共有できます。

Network Automation (NA) の統合

Network Automation (NA) の統合では、管理対象サーバーとこのサーバーに接続されたネットワークデバイスに関する詳細情報を精査します。これによりサーバーとデバイスの関係性を特定でき、それらの変更の調整と適用が可能になります。NAではSAとの統合をサポートがサポートされており、イベント履歴の統合、コンプライアンスの検証、サーバーやネットワークデバイスの重複検出などのアクションをデバイスグループ上で実行できます。

索引

す

そ

て

ひ

ふ

ほ

め

も